Программный комплекс Систэм Платформ

Подсистема SePlatform.Security 1.4

Руководство администратора

Редакция	Соответствует версии ПО
6	1.4.14

Содержание

1. О продукте ... **5**

2. Установка и удаление ... **7**

3. LDAP-сервер и его настройка ... **12**
3.1. Для пользователей Windows ... 12
3.1.1. Однонаправленное резервирование ... 13
3.1.2. Разнонаправленное резервирование ... 14
3.2. Для пользователей DEB-систем ... 16
3.2.1. Резервирование LDAP-сервера ... 21
3.2.1.1. Однонаправленное резервирование ... 21
3.2.1.2. Разнонаправленное резервирование ... 24
3.3. Для пользователей RPM-систем ... 27
3.3.1. Резервирование LDAP-сервера ... 31
3.3.1.1. Однонаправленное резервирование ... 31
3.3.1.2. Разнонаправленное резервирование ... 34

4. Агент безопасности и его настройка ... **38**

5. Запуск сервисов (для ОС Linux) ... **44**

6. Редактирование конфигурации на LDAP-сервере с помощью SecurityConfigurator ... **46**
6.1. Подключение к LDAP-серверу из SecurityConfigurator ... 47
6.2. Создание и редактирование групп пользователей ... 54
6.3. Создание и редактирование прав и приложений ... 57
6.4. Создание ролей ... 60
6.5. Создание и редактирование учетных записей ... 61
6.6. Назначение и указание значений прав ... 71
6.7. Организация кластерного рабочего места ... 75
6.8. Резервное копирование конфигурации ... 80

7. Аудит безопасности ... **82**

8. Контроль целостности файлов и папок ... **91**

9. Безопасность в компонентах Систэм Платформ ... **94**

10. Решение распространенных проблем ... **95**

11. Приложения ... **101**
Приложение A: Пример конфигурационного файла Агент SePlatform.Security ... 101
Приложение B: SCAN-коды клавиш ... 103
Приложение C: Параметры запуска SecurityConfigurator ... 107
Приложение D: Права стандартного приложения SePlatform.Security ... 109

История изменений ... **112**
1.4 ... 112
1.4.4 ... 112
1.4.5 ... 112
1.4.6 ... 112
1.4.7 ... 113
1.4.9 ... 113
1.4.10 ... 113

1.4.12 114
1.4.14 114
Изменения документации 114
Редакция 1 114
Редакция 2 114
Редакция 3 115
Редакция 4 115
Редакция 5 115
Редакция 6 115
1.3 116
1.3.5 116
Изменения документации 116
Редакция 2 116
Редакция 3 116

1. О продукте

SePlatform.Security - подсистема безопасности, позволяющая:

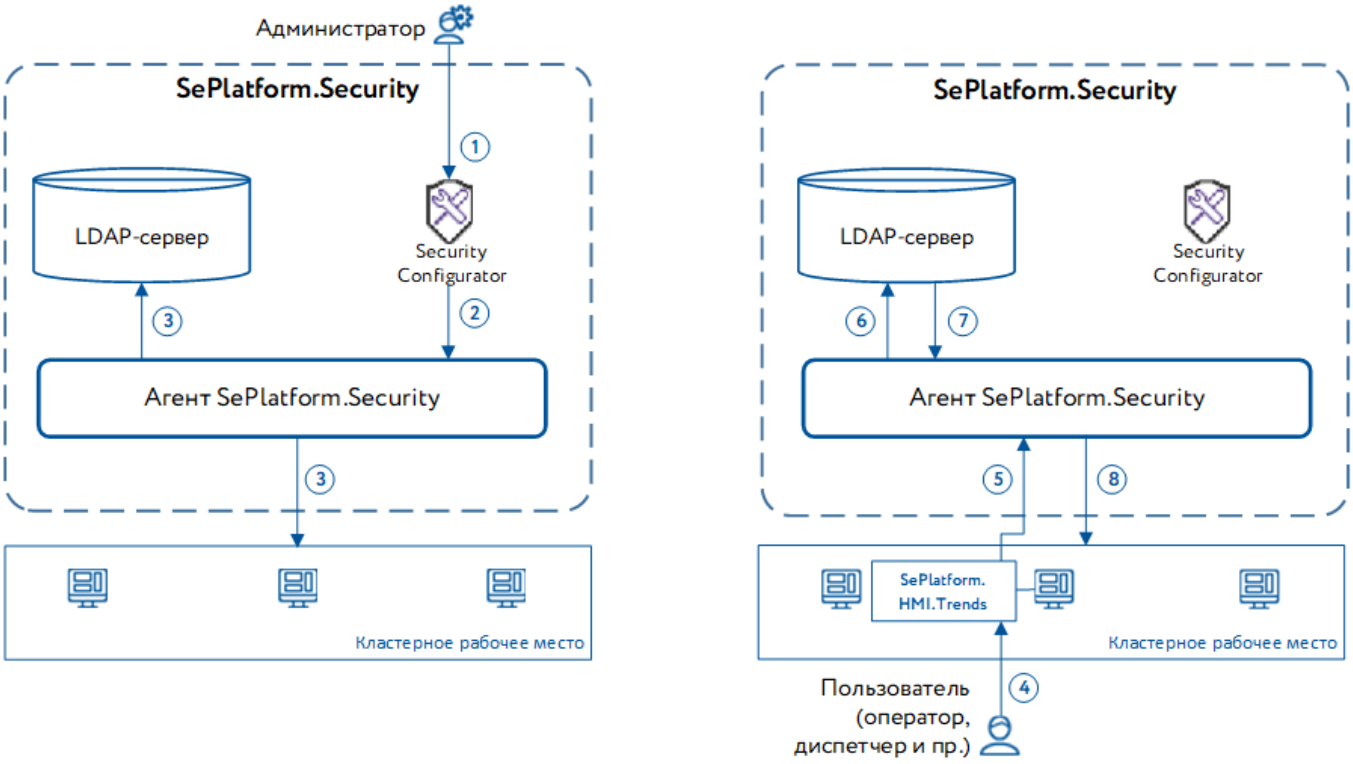
- разграничивать возможности пользователей в проектах автоматизации;
- вести аудит безопасности;
- контролировать целостность файлов и папок.

Подсистема безопасности SePlatform.Security состоит из компонентов:

- LDAP-сервер;
- агент безопасности;
- конфигуратор безопасности.

В качестве LDAP-сервера используется программа OpenLDAP. Агент безопасности представляет собой службу **`SePlatform.Security.Agent`** на ОС Windows или сервис **`seplatform.security.service`** на ОС Linux. В качестве конфигуратора можно использовать программу SecurityConfigurator, поставляемую вместе с дистрибутивом SePlatform.Security, либо SePlatform.HMI.SecurityConfigurator. Назначение, настройка и использование каждого компонента подробно описаны в отдельных разделах руководства.

На рисунке показаны примеры взаимодействия компонентов SePlatform.Security. На схеме слева описан процесс настройки подсистемы безопасности администратором (шаги 1-3), на схеме справа - процесс регистрации пользователя в подсистеме (шаги 4-8).



1. Администратор, используя конфигуратор безопасности (программу SecurityConfigurator), создает конфигурацию подсистемы безопасности. Предположим, создает учетную запись пользователя, назначает ему права, и объединяет несколько АРМ в кластерное рабочее место.
2. Эту информацию получает Агент SePlatform.Security.
3. Агент SePlatform.Security сохраняет полученную информацию на LDAP-сервере.

4. Предположим, пользователь, чья учетная запись создана администратором, собирается воспользоваться программой SePlatform.HMI.Trends, установленной на одном из АРМ кластерного рабочего места. SePlatform.HMI.Trends использует сервис безопасности. Поэтому пользователь должен зарегистрироваться в подсистеме безопасности. Для этого он вводит свои учетные данные в окне регистрации SePlatform.HMI.Trends.

5. SePlatform.HMI.Trends передает введенные учетные данные агенту безопасности.

6. Агент SePlatform.Security сравнивает введенные данные с информацией на LDAP-сервере.

7. Если введенные данные верны, сервер предоставляет агенту безопасности информацию о правах пользователя, назначенных ему администратором на шаге 1. Агент SePlatform.Security запоминает пользователя как текущего.

8. Агент SePlatform.Security предоставляет информацию о пользователе всем программам, использующим сервис безопасности, на всех АРМ кластерного рабочего места, куда у пользователя есть доступ.

2. Установка и удаление

Системные требования

Системные требования общие для всех компонентов подсистемы SePlatform.Security.

ОС	Microsoft Windows 10 Pro/11 Pro Microsoft Windows Server 2012/2012 R2/2016/2019/2022 Astra Linux, РЕД ОС, Ubuntu (glibc не ниже 2.17)
Разрядность ОС	x64
Процессор	Intel Celeron с тактовой частотой не менее 1.6 ГГц
Объем оперативной памяти	не менее 2 ГБ
Объем дисковой памяти	не менее 1 ГБ
Сетевой адаптер	Ethernet 10/100/1000 Мбит/с.
Установленное ПО	› SePlatform.Domain (обеспечивает работоспособность некоторых функций подсистемы) › антивирусное ПО › OPC Core Components версии 105.1 https://opcfoundation.org/developer-tools/samples-and-tools-classic/core-components/ › Microsoft .NET Framework 4.5 https://www.microsoft.com/ru-ru/download/details.aspx?id=30653

Также при использовании ОС Windows требуются:

Windows x64	› Microsoft Visual C++ 2015 (x86) Redistributable › Microsoft Visual C++ 2015 (x64) Redistributable https://www.microsoft.com/ru-ru/download/details.aspx?id=48145

Установка, удаление и восстановление для Windows

Компоненты подсистемы безопасности SePlatform.Security устанавливаются единовременно.

Для установки, удаления или восстановления SePlatform.Security запустите установочный файл `seplatform.security-<lng>-<arch>-<version>.msi`. Следуйте инструкциям мастера.

ПРИМЕЧАНИЕ

В названии файла `<lng>` - это язык продукта, `<arch>` - целевая процессорная архитектура, `<version>` - версия продукта.

ОБРАТИТЕ ВНИМАНИЕ

При установке OpenLDAP будет предложено придумать и ввести пароль администратора LDAP-сервера. Если пропустить этот шаг, будет назначен стандартный пароль **«secret»**.

После установки Агент SePlatform.Security функционирует в виде службы Windows **SePlatform.Security.Agent**.

Установка и удаление для Linux

Компоненты подсистемы безопасности SePlatform.Security устанавливаются по отдельности.

ОБРАТИТЕ ВНИМАНИЕ

Для Linux SecurityConfigurator не разработан. Для редактирования конфигурации на LDAP-сервере можно:

- либо подключаться к LDAP-серверу, развернутому на Linux, из SecurityConfigurator, установленном на Windows;
- либо использовать SePlatform.HMI.SecurityConfigurator. Подробнее об установке и использовании этого компонента - в соответствующем документе.

Установка и удаление Агент SePlatform.Security

Для установки Агент SePlatform.Security:

1. Вызовите пакет с командой на установку:
   - rpm-пакет:

     ```
     sudo rpm -i seplatform.security-<version>.<type>
     ```

   - deb-пакет:

     ```
     sudo dpkg -i seplatform.security-<version>.<type>
     ```

   После установки Агент SePlatform.Security функционирует в виде сервиса **seplatform.security.service**.
2. Запустите сервис агента безопасности:

   ```
   sudo systemctl start seplatform.security
   ```

   И сервис, обслуживающий пользовательские сессии - **seplatform.security.useractivity.service**. Прежде чем запустить сервис, его необходимо настроить. Как это сделать, описано в разделе 5. Запуск сервисов (для ОС Linux) (стр. 44).

   Проверить состояние сервиса агента безопасности можно командой (должна быть активна):

   ```
   sudo systemctl status seplatform.security
   ```

3. Разрешите сервису стартовать при запуске ОС:

   ```
   sudo systemctl enable seplatform.security
   ```

4. После установки выполните импорт настроек модуля мониторинга, как описано ниже.

Для удаления Агент SePlatform.Security вызовите команду на удаление:

- rpm-пакет:

```
sudo rpm -e seplatform.security
```

- deb-пакет:

```
sudo dpkg -r seplatform.security
```

Импорт настроек модулей мониторинга

Эту настройку необходимо выполнить для того, чтобы модули мониторинга отслеживали длительность сессий и блокировок пользователей.

1. Перейдите в папку установки SePlatform.Security:

```
cd /opt/SePlatform/SePlatform.Security
```

2. Примените настройки модулей с помощью команды:

```
sudo sh ./monitor.export.sh
sudo sh ./addLockTime.sh
```

Установка и удаление OpenLDAP

Чтобы установить OpenLDAP:

1. Скачайте и установите пакеты OpenLDAP, запустив команду:
   - для rpm-систем:

```
sudo yum install openldap openldap-servers
```

   - для deb-систем:

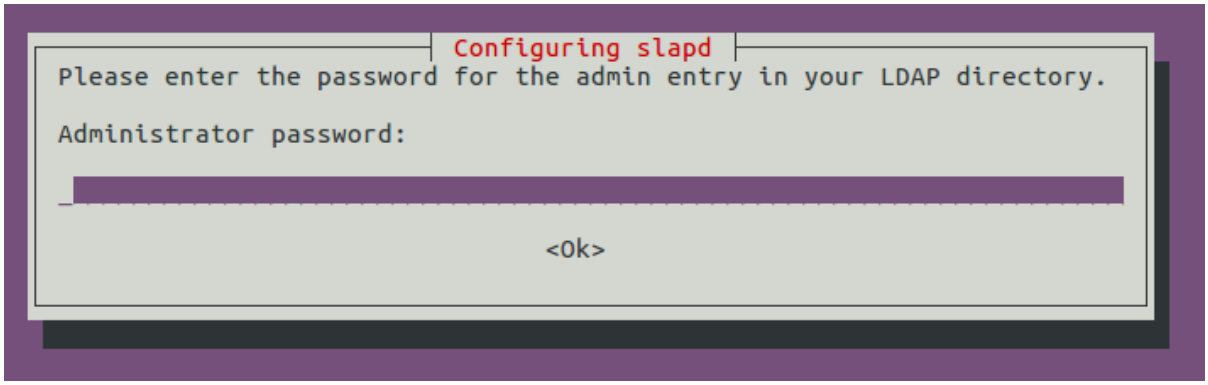
```
sudo apt install slapd ldap-utils
```

   Для скачивания пакетов необходимо подключение к интернету.

ОБРАТИТЕ ВНИМАНИЕ

В ходе установки, в зависимости от ОС, может быть создана учетная запись администратора OpenLDAP (**«admin»**). Тогда будет предложено задать пароль учетной записи администратора. Задайте пароль, например, **«secret»**. Если учетная запись не будет создана автоматически, её необходимо будет создать вручную, как описано в разделе3. LDAP-сервер и его настройка (стр. 12).

Ниже приведен внешний вид окна ввода пароля создаваемой учетной записи администратора OpenLDAP для Ubuntu.



2. Запустите сервис **OpenLDAP Service**:

```
sudo systemctl start slapd
```

Проверить состояние сервиса можно командой (должна быть активна):

```
sudo systemctl status slapd
```

3. Разрешите сервису стартовать при запуске ОС:

```
sudo systemctl enable slapd
```

4. Разрешите запросы к демону LDAP-сервера через брандмауэр:

- для rpm-систем:

```
sudo firewall-cmd --add-service=ldap
```

- для deb-систем:

```
sudo ufw allow ldap
```

ВАЖНО

После установки перейдите к настройке LDAP-сервера.

Чтобы удалить OpenLDAP, вызовите команду на удаление:

```
sudo apt-get purge slapd ldap-utils
```

Эта команда удалит OpenLDAP, но его настройки и резервные копии баз останутся. Чтобы удалить их, выполните команды:

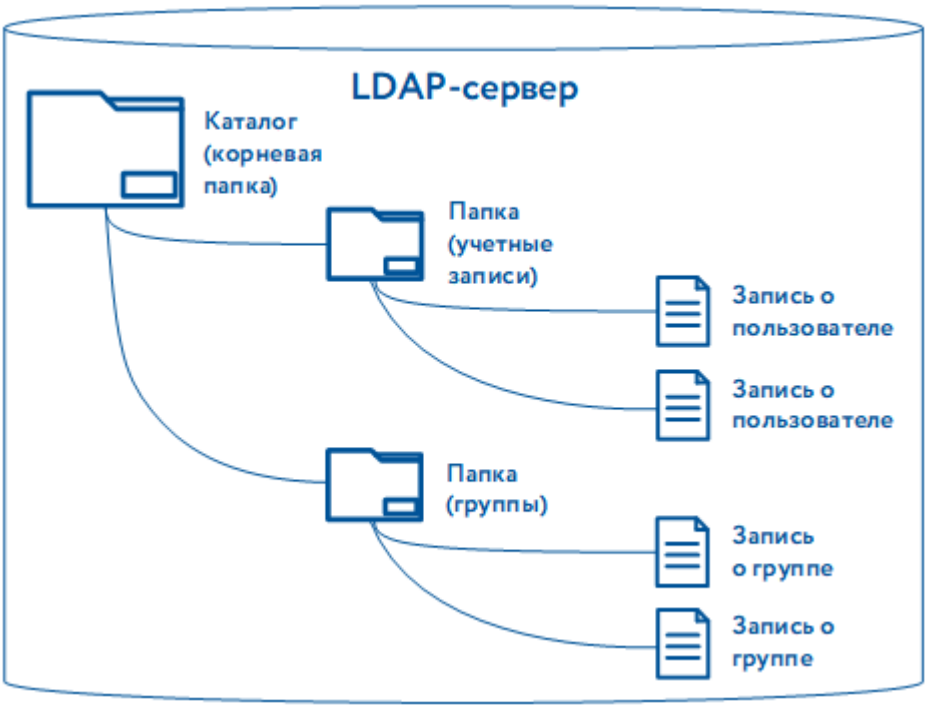
```
sudo rm -rf /etc/ldap/slapd.d/*
sudo rm -rf /var/lib/ldap/*
sudo rm -rf /var/backups/*
```

3. LDAP-сервер и его настройка

Подсистема безопасности SePlatform.Security построена на протоколе доступа к описанным каталогам - LDAP. Подробнее о протоколе LDAP можно прочитать по ссылке. LDAP-сервер - это хранилище каталогов LDAP. Каталоги предназначены для хранения записей об:

- учетных записях пользователей;
- группах пользователей;
- правах и приложениях, в которые объединяются права;
- рабочих местах и станциях.

Каталог имеет вид дерева: корневой узел содержит записи, которые могут быть объединены в папки.



В качестве LDAP-сервера SePlatform.Security использует продукт OpenLDAP.

Редактирование конфигурации на LDAP-сервере тоже выполняется по-разному. Чтобы создать или редактировать конфигурацию, нужно подключиться к LDAP-серверу:

- на Windows для этого можно использовать и SecurityConfigurator, и SePlatform.HMI.SecurityConfigurator;
- на Linux можно:
  - либо использовать SePlatform.HMI.SecurityConfigurator;
  - либо подключиться к OpenLDAP, установленному на Linux, из SecurityConfigurator, установленном на Windows. Процесс подключения описан в 6.1. Подключение к LDAP-серверу из SecurityConfigurator (стр. 47).

3.1. Для пользователей Windows

Настройка OpenLDAP зачастую не требуется.

LDAP-сервер можно резервировать. Резервирование (репликация) LDAP-сервера позволяет синхронизировать конфигурации двух и более серверов. Резервирование может быть:

- однонаправленным - в этом случае конфигурация одного сервера (поставщика) тиражируется на другие сервера (приемники);
- разнонаправленным - в этом случае синхронизируются конфигурации нескольких серверов.

ВАЖНО

Прежде чем перейти к настройке резервирования, сохраните бэкап конфигурации и БД резервируемых серверов. Для этого скопируйте куда-либо файлы `data.mdb` и `lock.mdb`, расположенные в папке `C:\Program Files\OpenLDAP\data`. В случае ошибок резервирования восстановите бэкап, заменив содержимое папки скопированными ранее файлами.

3.1.1. Однонаправленное резервирование

Чтобы настроить однонаправленное резервирование:

1. Определите, какой из LDAP-серверов будет поставщиком, а какие - приемниками.
2. Настройте сервер-поставщик:
   2.1. Перейдите к файлу конфигурации OpenLDAP `slapd.conf`, расположенному в папке `C:\ProgramData\OpenLDAP\openldap` компьютера, где установлен сервер-поставщик. Раскомментируйте конструкцию syncprov:

```
#overlay syncprov
#syncprov-checkpoint 100 10
#syncprov-sessionlog 100
#index entryCSN eq
#index entryUUID eq
```

   2.2. Перезапустите службу **`OpenLDAP Service`**.

3. Настройте сервера-приемники:

ОБРАТИТЕ ВНИМАНИЕ

Описанные ниже действия выполните на каждом из серверов-приемников.

3.1. Перейдите к файлу конфигурации OpenLDAP `slapd.conf`, расположенному в папке `C:\ProgramData\OpenLDAP\openldap` компьютера, где установлен сервер-приемник. Раскомментируйте конструкцию syncrepl:

```
#syncrepl rid=1
#      provider=ldap://172.16.13.167:389
#      type=refreshAndPersist
#      retry="60 10 300 +"
#      searchbase="dc=maxcrc,dc=com"
#      filter="(objectClass=*)"
#      scope=sub
#      attrs="*,+"
#      schemachecking=off
#      bindmethod=simple
#      sizelimit=2147483648
#      timelimit=2147483648
#updateref ldap://172.16.13.167:389
```

3.2. Укажите IP-адрес и порт сервера-поставщика в значениях параметров provider и updateref вместо значения по умолчанию **«172.16.13.167:389»**.

3.3. Перезапустите службу **OpenLDAP Service**.

3.4. Повторите описанные в пункте действия на всех серверах-приемниках.

4. Настройте Агент SePlatform.Security:

4.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `C:\Program Files\SePlatform\SePlatform.Security` или `C:\Program Files (x86)\SePlatform\SePlatform.Security`. Вложите в элемент `<LdapHosts>` элементы `<LDAPServer>` с IP-адресами и портами всех подчиненных серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="199.99.99.111" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

4.2. Перезапустите службу **SePlatform.Security.Agent**.

3.1.2. Разнонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Отключите все возможные репликации баз и серверов.
2. Убедитесь, что содержимое баз резервируемых серверов идентично.
3. Остановите все программы, взаимодействующие с серверами OpenLDAP.
4. Убедитесь, что системное время резервируемых серверов одинаковое, иначе синхронизация изменений будет работать в одну сторону.

5. На время настройки резервирования одного из серверов остановите остальные резервируемые сервера OpenLDAP.

ОБРАТИТЕ ВНИМАНИЕ

Описанные ниже действия выполните на каждом из резервируемых серверов.

Чтобы настроить разнонаправленное резервирование:

1. Измените файл конфигурации OpenLDAP `slapd.conf`, расположенный в папке `C:\ProgramData\OpenLDAP\openldap`, следующим образом:

1.1. Перед определением базы добавьте уникальный идентификатор сервера:

```
#######################################################################
# mdb database definitions
#######################################################################

ServerID 001

database        mdb
suffix          "dc=maxcrc,dc=com"
rootdn          "cn=Manager,dc=maxcrc,dc=com"
```

ОБРАТИТЕ ВНИМАНИЕ

ServerID должен быть уникальным для каждого сервера.

1.2. Раскомментируйте всю конструкцию syncrepl, кроме последней строки:

```
syncrepl rid=1
        provider=ldap://172.16.13.167:389
        type=refreshAndPersist
        retry="60 10 300 +"
        searchbase="dc=maxcrc,dc=com"
        filter="(objectClass=*)"
        scope=sub
        attrs="*,+"
        schemachecking=off
        bindmethod=simple
        sizelimit=2147483648
        timelimit=2147483648
#updateref ldap://172.16.13.167:389
```

Конструкция syncrepl описывает один из резервируемых серверов. Добавьте столько конструкций syncrepl, сколько серверов участвуют в резервировании помимо текущего.

ОБРАТИТЕ ВНИМАНИЕ

Внутри одного сервера параметры rid разных конструкций syncrepl должны иметь уникальные значения.

1.3. В каждой конструкции syncrepl укажите IP-адрес и порт сервера, который она описывает. Для этого в строке параметра provider замените по умолчанию **«172.16.13.167:389»** на нужное значение.

1.4. В конце файла добавьте запись:

```
mirrormode TRUE
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
index entryCSN eq
index entryUUID eq
```

2. Перезапустите службу **OpenLDAP Service**.
3. Повторите описанные выше действия на каждом из резервируемых серверов.
4. Настройте Агент SePlatform.Security:

4.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `C:\Program Files\SePlatform\SePlatform.Security` или `C:\Program Files (x86)\SePlatform\SePlatform.Security`. Вложите в элемент `<LdapHosts>` элементы `<LDAPServer>` с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="199.99.99.111" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

4.2. Перезапустите службу **SePlatform.Security.Agent**.

После настройки последовательно включите все сервера OpenLDAP. Подключитесь напрямую к каждой базе и убедитесь, что ошибок не возникло. Для проверки внесите изменения в конфигурацию на одном из серверов. Убедитесь, что эти изменения появились и на других серверах.

3.2. Для пользователей DEB-систем

Для настройки LDAP-сервера необходимо последовательно выполнить все шаги, описанные в данном разделе.

ОБРАТИТЕ ВНИМАНИЕ

Все команды настройки OpenLDAP необходимо выполнять от имени суперпользователя root. Для этого перед вводом команды настройки введите команду `sudo`.

Создать учетную запись администратора LDAP-сервера

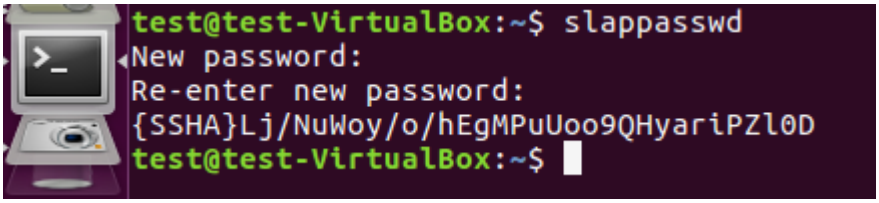
Если при установке OpenLDAP (стр. 10) учетная запись была создана, и для нее нужно было придумать пароль, этот шаг можно пропустить и перейти к следующему пункту Переименовать домен базы данных LDAP (стр. 19).

1. Сгенерируйте шифрованное значение пароля для учетной записи администратора с помощью команды:

```
slappasswd
```

ПРИМЕР

Шифрованное значение имеет вид {SSHA}строка_символов.



ОБРАТИТЕ ВНИМАНИЕ

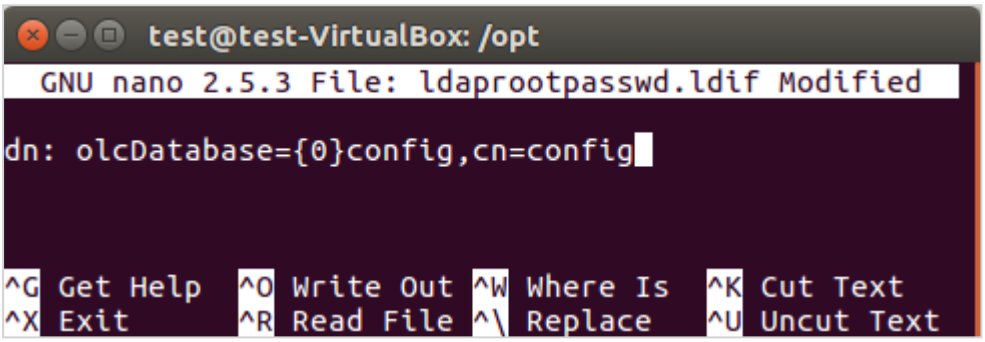
Сохраните полученное значение для следующих шагов настройки.

2. Затем создайте файл `ldaprootpasswd.ldif`, который используется для добавления учетной записи администратора в каталог LDAP:

```
sudo nano ldaprootpasswd.ldif
```

ПРИМЕЧАНИЕ

В данном примере для создания и редактирования текстовых файлов на ОС Linux предлагается использовать редактор NANO. Команда `nano` позволяет открыть существующий или создать новый файл с указанным именем. В результате вызова команды файл откроется в соответствующем редакторе.



Если используете редактор NANO, то:

- чтобы сохранить файл, нажмите сочетание клавиш **Ctrl** + **O**;
- чтобы выйти из редактора, нажмите сочетание клавиш **Ctrl** + **X**;
- чтобы вызвать справку, нажмите сочетание клавиш **Ctrl** + **G**.

Добавьте в файл следующее:

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}строка_символов
```

- olcDatabase - указывает конкретное имя экземпляра базы данных и обычно находится в `/etc/ldap/slapd.d/cn=config`;
- cn=config - указывает глобальные параметры конфигурации;
- {SSHA}строка_символов - шифрованное значение пароля.

Затем сохраните файл, нажав сочетание клавиш **Ctrl** + **O**, и выйдите из редактора, нажав сочетание клавиш **Ctrl** + **X**.

3. Добавьте запись администратора в LDAP командой, указав URI со ссылкой на LDAP-сервер и файл, созданный выше:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f ldaprootpasswd.ldif
```

Переименовать домен базы данных LDAP

При установке OpenLDAP в качестве имени домена по умолчанию используется значение **«nodomain»**. Значение имени домена по умолчанию для компонентов SePlatform.Security - **«maxcrc.com»**. Эту настройку обязательно нужно выполнить.

Чтобы изменить имя домена, используйте команду:

```
sudo dpkg-reconfigure slapd
```

В открывшемся окне на вопрос **Не выполнять настройку сервера OpenLDAP?** ответьте **«No»**. Запустится конфигуратор LDAP-сервера. В конфигураторе:

- в качестве имени домена задайте строку **«maxcrc.com»**;
- название организации укажите произвольное;
- затем укажите пароль администратора дважды;
- оставьте значение типа папки `/var/lib/ldap` по умолчанию - **«mdb»**;
- оставьте протокол по умолчанию - **«ldap.v3»**;
- на вопрос **Удалять базу данных при удалении slapd?** ответьте так, как считаете нужным;
- на вопрос **Переместить старую базу данных?** ответьте **«Да»**, если есть файлы старой базы данных.

Затем перезапустите сервис **OpenLDAP Service**:

```
sudo systemctl restart slapd
```

Определить структуру каталогов на LDAP-сервере

После установки OpenLDAP структура каталогов на сервере еще не определена. Эту настройку обязательно нужно выполнить.

Чтобы сформировать структуру данных внутри каталогов LDAP, нужно применить файлы схемы. Необходимые файлы схемы `seplatform.security.ldif` и shell-скрипт `seplatform.security.schema.export.sh` устанавливаются вместе с пакетом SePlatform.Security.

1. Для применения схемы выполните следующие команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./seplatform.security.schema.export.sh
```

Примененную схему можно увидеть по команде:

```
sudo ls -la /etc/ldap/slapd.d/cn=config/cn=schema/
```

2. Перезапустите сервис **`OpenLDAP Service`**:

```
sudo systemctl restart slapd
```

3. Для проверки можно подключиться к OpenLDAP из программы LdapAdmin.exe. При подключении укажите следующие параметры:

- Host: **«127.0.0.1»** (либо укажите нужный IP-адрес сервера), Port: **«389»**, Version: **«3»**.
- Base: **«dc=maxcrc,dc=com»**.
- Установите галочку на **`Simple authentication`**, остальные снимите.
- Account Username: **«cn=admin,dc=maxcrc,dc=com»**.
- Password: **«secret»** (либо указанный при установке).

Добавить шаблон политики контроля доступа

Чтобы содержимое каталогов можно было просматривать и редактировать, нужно настроить политики контроля доступа. Для этого следует создать файл-шаблон с описанием прав доступа к OpenLDAP и применить его.

ПРИМЕЧАНИЕ

Файл, создаваемый в инструкции, для анонимных пользователей делает доступным чтение, для зарегистрированных пользователей - редактирование каталогов.

1. Создайте файл-шаблон `access.ldif` со следующим содержанием:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by users write by * read
```

2. Примените созданный файл-шаблон командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f access.ldif
```

Создать каталог на LDAP-сервере

Чтобы начать создавать учетные записи пользователей, объединять их в группы и наделять правами, нужно создать каталог на LDAP-сервере, в котором будет храниться создаваемая конфигурация.

Процесс создания нового каталога на LDAP-сервере и подключения к нему описан в разделе 6.1. Подключение к LDAP-серверу из SecurityConfigurator (стр. 47). SecurityConfigurator может быть установлен только на Windows. Обратите внимание, что в таком случае оба компьютера - с Windows и с Linux - должны быть объединены в сеть SePlatform.Net. Подробнее о том, как объединить компьютеры в сеть, можно прочитать в 6.7. Организация кластерного рабочего места (стр. 75), или в документе на SePlatform.Domain. Если возможности использовать SecurityConfigurator на Windows нет, на АРМ с Linux можно установить SePlatform.HMI.SecurityConfigurator. Подробнее о том, как использовать этот конфигуратор и создавать в нем каталоги, читайте в соответствующем документе.

3.2.1. Резервирование LDAP-сервера

Резервирование (репликация) LDAP-сервера позволяет синхронизировать конфигурации двух и более серверов. Резервирование может быть:

- однонаправленным - в этом случае конфигурация одного сервера (поставщика) тиражируется на другие сервера (приемники);
- разнонаправленным - в этом случае синхронизируются конфигурации нескольких серверов.

3.2.1.1. Однонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Убедитесь, что типы баз данных всех серверов - **«mdb»**, с помощью команды:

```
sudo slapcat -n0
```

> ОБРАТИТЕ ВНИМАНИЕ
>
> Если тип БД отличается, то во всех дальнейших командах нужно заменить **«mdb»** на текущий тип БД.

2. Сделайте бэкап конфигурации и БД сервера-поставщика в текущей папке с помощью команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

Чтобы настроить однонаправленное резервирование:

1. Определите, какой из LDAP-серверов будет поставщиком, а какие - приемниками.
2. Настройте сервера-приемники:

ОБРАТИТЕ ВНИМАНИЕ

Описанные в пункте действия выполните на каждом из серверов-приемников.

2.1. Ознакомьтесь с файлом `openldap-enable-syncrepl-consumer.ldif`, устанавливаемым в составе SePlatform.Security:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
#delete: olcSyncrepl
add: olcSyncrepl
olcSyncrepl:
  rid=001
  provider=ldap://192.168.56.1
  binddn="cn=admin,dc=maxcrc,dc=com"
  bindmethod=simple
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  type=refreshAndPersist
  timeout=0
  network-timeout=0
  retry="60 +"

dn: olcDatabase={1}mdb,cn=config
changetype: modify
#delete: olcUpdateRef
add: olcUpdateRef
olcUpdateRef: ldap://192.168.56.1
```

Обратите внимание, что отступ в каждой строке внутри конструкции olcSyncRepl обязательно должен содержать по два пробела.

2.2. Измените следующие строки:

- **«dn: olcDatabase={1}mdb,cn=config»** - замените **«mdb»** на текущий тип БД, если он отличается;
- **«provider=ldap://192.168.56.1»** - замените значение по умолчанию **«192.168.56.1»** на адрес сервера-поставщика данных;
- **«credentials="secret"»** - если меняли пароль администратора OpenLDAP, замените **«secret»** на актуальное значение;
- **«olcUpdateRef: ldap://192.168.56.1»** - замените значение по умолчанию **«192.168.56.1»** на адрес сервера-поставщика данных.

ОБРАТИТЕ ВНИМАНИЕ

В файлах `.ldif` порядок и количество пробелов имеют важное значение.

2.3. Для применения внесенных изменений выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-enable-syncrepl-consumer.sh
```

2.4. Перезапустите сервис **OpenLDAP Service**:

```
sudo systemctl restart slapd
```

3. Настройте сервер-поставщик:

3.1. Ознакомьтесь с файлом `openldap-enable-syncrepl-provider.ldif`, устанавливаемым в составе SePlatform.Security:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpCheckpoint: 100 10
olcSpSessionlog: 100

dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq
```

3.2. Замените **«mdb»** на текущий тип БД, если он отличается, в строках:

- **«dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config»**;
- **«dn: olcDatabase={1}mdb,cn=config»**,

3.3. Для применения внесенных изменений выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-enable-syncrepl-provider.sh
```

3.4. Перезапустите сервис **OpenLDAP Service**:

```
sudo systemctl restart slapd
```

4. Настройте Агент SePlatform.Security:

4.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `/opt/SePlatform/SePlatform.Security`. Добавьте в секцию элемента `<LdapHosts>` строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

В данном примере:

- **«127.0.0.1»** - адрес локального сервера (поставщика);
- **«172.16.13.167»** - пример адреса сервера-приемника (укажите нужный адрес).

4.2. Перезапустите сервис:

```
sudo systemctl restart seplatform.security.service
```

3.2.1.2. Разнонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Убедитесь, что типы баз данных всех серверов - **«mdb»**, с помощью команды:

```
sudo slapcat -n0
```

> ОБРАТИТЕ ВНИМАНИЕ
>
> Если тип БД отличается, то во всех дальнейших командах нужно заменить **«mdb»** на текущий тип БД.

2. Отключите все возможные репликации баз и серверов.
3. Убедитесь, что содержимое баз резервируемых серверов идентично.
4. Сделайте бэкап конфигурации с помощью команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

5. Остановите все программы, взаимодействующие с серверами OpenLDAP.
6. Убедитесь, что системное время резервируемых серверов одинаковое, иначе синхронизация изменений будет работать в одну сторону.
7. На время настройки резервирования одного из серверов остановите остальные резервируемые сервера OpenLDAP.

Чтобы настроить разнонаправленное резервирование:

1. На любом из резервируемых серверов создайте файл конфигурации `openldap-enable-syncrepl-multiprovider-server.ldif` со следующим содержанием:

```
###############################################################
# Check/modify database type (bdb/hdb/mbd/...), server ID (unique number),
# address of provider, binddn, credentials, searchbase.
###############################################################

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: syncprov.la

###############################################################

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100

###############################################################

dn: cn=config
changetype: modify
replace: olcServerID
olcServerID: 1

dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl:
  rid=001
  provider=ldap://192.168.56.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
olcSyncRepl:
  rid=002
  provider=ldap://192.168.57.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
```

```
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
-
add: olcMirrorMode
olcMirrorMode: TRUE

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Обратите внимание, что отступ в каждой строке внутри конструкции olcSyncRepl обязательно должен содержать по два пробела.

2. Измените файл конфигурации следующим образом:

   2.1. В строке olcServerID: 1 придумайте и укажите идентификатор сервера;

   > ОБРАТИТЕ ВНИМАНИЕ
   > olcServerID должен быть уникальным для каждого резервируемого сервера.

   2.2. Замените **«mdb»** на текущий тип БД, если он отличается, в строках:

   - **«dn: olcDatabase={1}mdb,cn=config»**;
   - **«dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config»**

   2.3. Добавьте столько конструкций olcSyncRepl, сколько серверов участвуют в резервировании помимо текущего. Каждая конструкция olcSyncRepl описывает один из резервируемых серверов.

   > ОБРАТИТЕ ВНИМАНИЕ
   > Внутри одного сервера параметры rid разных конструкций olcSyncRepl должны иметь уникальные значения.

   2.4. В каждой конструкции olcSyncRepl укажите IP-адрес и порт сервера, который она описывает, в строке параметра provider.

3. Для применения внесенных изменений выполните команду:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f openldap-enable-syncrepl-
multiprovider-server.ldif
```

4. Перезапустите сервер:

```
sudo systemctl restart slapd
```

5. Повторите все описанные действия на каждом из резервируемых серверов.

6. Настройте Агент SePlatform.Security:

6.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `/opt/SePlatform/SePlatform.Security`. Добавьте в секцию элемента `<LdapHosts>` строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

В данном примере:

- **«127.0.0.1»** - адрес локального сервера (поставщика);
- **«172.16.13.167»** - пример адреса сервера-приемника (укажите нужный адрес).

6.2. Перезапустите сервис:

```
sudo systemctl restart seplatform.security.service
```

После настройки последовательно включите все сервера OpenLDAP. Подключитесь напрямую к каждой базе и убедитесь, что ошибок не возникло. Для проверки внесите изменения в конфигурацию на одном из серверов. Убедитесь, что эти изменения появились и на других серверах.

3.3. Для пользователей RPM-систем

ОБРАТИТЕ ВНИМАНИЕ

Все команды настройки OpenLDAP необходимо выполнять от имени суперпользователя root. Для этого перед вводом команды настройки введите команду `sudo`.

Предварительно:

1. Установите клиентское приложение, необходимое для доступа и изменения каталогов OpenLDAP.

```
sudo yum install openldap-clients
```

2. Проверьте имя и тип базы данных (hdb, mdb, и т.п.) с помощью команды:

```
sudo slapcat -n0
```

Пример искомого значения: **«dn: olcDatabase={2}mdb,cn=config»**. Если база имеет тип, отличный от **«{2}mdb»**, во всех файлах, создаваемых и применяемых в инструкции ниже, следует указывать правильный тип базы.

Создайте учетную запись администратора LDAP-сервера.

1. Сгенерируйте шифрованное значение пароля для учетной записи администратора с помощью команды:

```
slappasswd
```

Шифрованное значение имеет вид {SSHA}строка_символов. Сохраните полученное значение для следующих шагов настройки.

2. Затем в папке `/opt/SePlatform` создайте файл-схему LDIF `config.ldif`, который используется для добавления учетной записи администратора в каталог LDAP:

```
sudo nano config.ldif
```

ПРИМЕЧАНИЕ

В данном примере для создания и редактирования текстовых файлов на ОС Linux предлагается использовать редактор NANO. Команда `nano` позволяет открыть существующий или создать новый файл с указанным именем. В результате вызова команды файл откроется в соответствующем редакторе.

Если используете редактор NANO, то:

- чтобы сохранить файл, нажмите сочетание клавиш **Ctrl** + **O**;
- чтобы выйти из редактора, нажмите сочетание клавиш **Ctrl** + **X**;
- чтобы вызвать справку, нажмите сочетание клавиш **Ctrl** + **G**.

Добавьте в файл следующее:

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}строка_символов
```

- olcDatabase - указывает конкретное имя экземпляра базы данных и обычно находится в `/etc/ldap/slapd.d/cn=config`;
- cn=config - указывает глобальные параметры конфигурации;
- {SSHA}строка_символов - шифрованное значение пароля администратора.

Затем сохраните файл, нажав сочетание клавиш **Ctrl** + **O**, и выйдите из редактора, нажав сочетание клавиш **Ctrl** + **X**.

3. Добавьте запись администратора в LDAP командой, указав URI со ссылкой на LDAP-сервер и файл, созданный выше:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f config.ldif
```

В случае успешного завершения операции должно появиться следующее сообщение:

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

Чтобы содержимое каталогов можно было просматривать и редактировать, нужно настроить политики контроля доступа. Для этого следует создать файл-шаблон с описанием прав доступа к OpenLDAP и применить его.

ПРИМЕЧАНИЕ

Файл, создаваемый в инструкции, для анонимных пользователей делает доступным чтение, для зарегистрированных пользователей - редактирование каталогов.

1. Создайте файл-шаблон `access.ldif` со следующим содержанием:

```
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by users write by * read
```

2. Примените созданный файл-шаблон командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f access.ldif
```

В случае успешного завершения операции должно появиться следующее сообщение:

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}mdb,cn=config"
```

Для следующей настройки снова потребуется создать файл-схему и применить его.

1. Создайте файл `db.ldif`.

```
sudo nano db.ldif
```

2. Добавьте в файл следующее:

```
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}строка_символов
```

где {SSHA}строка_символов - шифрованное значение пароля администратора.

3. Примените созданный файл командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f db.ldif
```

В случае успешного завершения операции должно появиться следующее сообщение:

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}mdb,cn=config"

modifying entry "olcDatabase={2}mdb,cn=config"

modifying entry "olcDatabase={2}mdb,cn=config"
```

Теперь необходимо применить файлы-схемы, поставляющиеся вместе с OpenLDAP.

1. Перейдите к папке, где хранятся файлы.

```
cd /etc/openldap/schema/
```

2. Затем примените файлы-схемы в том порядке, в котором они перечислены ниже.

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f collective.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f corba.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cosine.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f duaconf.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f dyngroup.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f inetorgperson.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f java.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f misc.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f nis.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f openldap.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f pmi.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ppolicy.ldif
```

После выполнения каждой команды должно появляться сообщение об успешном применении схемы:

```
adding new entry "cn=ppolicy,cn=schema,cn=config"
```

Далее необходимо применить схему, поставляемую вместе с дистрибутивом SePlatform.Security.

1. Вернитесь в каталог агента безопасности.

```
cd /opt/SePlatform/SePlatform.Security
```

2. Примените здесь файл-схему `seplatform.security`.

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f seplatform.security.ldif
```

Теперь необходимо создать и применить файл-схему, где будет указан так называемый домен, в котором функционирует агент безопасности.

1. Перейдите к каталогу на уровень выше.

```
cd /opt/SePlatform
```

2. Создайте файл-схему `empty.ldif`.

```
sudo nano empty.ldif
```

3. Добавьте в файл следующее:

```
dn: dc=maxcrc,dc=com
objectClass: domain
objectClass: top
dc: maxcrc
```

4. Примените созданный файл командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f empty.ldif
```

Теперь сервер OpenLDAP настроен. Чтобы начать создавать учетные записи пользователей, объединять их в группы и наделять правами, нужно создать каталог на LDAP-сервере, в котором будет храниться создаваемая конфигурация.

Процесс создания нового каталога на LDAP-сервере и подключения к нему описан в разделе 6.1. Подключение к LDAP-серверу из SecurityConfigurator (стр. 47). SecurityConfigurator может быть установлен только на Windows. Обратите внимание, что в таком случае оба компьютера - с Windows и с Linux - должны быть объединены в сеть SePlatform.Net. Подробнее о том, как объединить компьютеры в сеть, можно прочитать в 6.7. Организация кластерного рабочего места (стр. 75), или в документе на SePlatform.Domain. Если возможности использовать SecurityConfigurator на Windows нет, на АРМ с Linux можно установить SePlatform.HMI.SecurityConfigurator. Подробнее о том, как использовать этот конфигуратор и создавать в нем каталоги, читайте в соответствующем документе.

3.3.1. Резервирование LDAP-сервера

Резервирование (репликация) LDAP-сервера позволяет синхронизировать конфигурации двух и более серверов. Резервирование может быть:

- однонаправленным - в этом случае конфигурация одного сервера (поставщика) тиражируется на другие сервера (приемники);
- разнонаправленным - в этом случае синхронизируются конфигурации нескольких серверов.

3.3.1.1. Однонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Убедитесь, что типы баз данных всех серверов - **«mdb»**, с помощью команды:

```
sudo slapcat -n0
```

Пример искомого значения: **«dn: olcDatabase={2}mdb,cn=config»**. Если база имеет тип, отличный от **«{2}mdb»**, во всех файлах, создаваемых и применяемых в инструкции ниже, следует указывать правильный тип базы.

2. Сделайте бэкап конфигурации и БД сервера-поставщика в текущей папке с помощью команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

Чтобы настроить однонаправленное резервирование:

1. Определите, какой из LDAP-серверов будет поставщиком, а какие - приемниками.
2. Настройте сервера-приемники:

ОБРАТИТЕ ВНИМАНИЕ

Описанные в пункте действия выполните на каждом из серверов-приемников.

2.1. Ознакомьтесь с файлом `openldap-enable-syncrepl-consumer.ldif`, устанавливаемым в составе SePlatform.Security:

```
dn: olcDatabase={2}mdb,cn=config
changetype: modify
#delete: olcSyncrepl
add: olcSyncrepl
olcSyncrepl:
  rid=001
  provider=ldap://192.168.56.1
  binddn="cn=admin,dc=maxcrc,dc=com"
  bindmethod=simple
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  type=refreshAndPersist
  timeout=0
  network-timeout=0
  retry="60 +"

dn: olcDatabase={2}mdb,cn=config
changetype: modify
#delete: olcUpdateRef
add: olcUpdateRef
olcUpdateRef: ldap://192.168.56.1
```

Обратите внимание, что отступ в каждой строке внутри конструкции olcSyncRepl обязательно должен содержать по два пробела.

2.2. Измените следующие строки:

- **«dn: olcDatabase={2}mdb,cn=config»** - замените **«{2}mdb»** на текущий тип БД, если он отличается;
- **«provider=ldap://192.168.56.1»** - замените значение по умолчанию **«192.168.56.1»** на адрес сервера-поставщика данных;
- **«credentials="secret"»** - если меняли пароль администратора OpenLDAP, замените **«secret»** на актуальное значение;
- **«olcUpdateRef: ldap://192.168.56.1»** - замените значение по умолчанию **«192.168.56.1»** на адрес сервера-поставщика данных.

ОБРАТИТЕ ВНИМАНИЕ

В файлах `.ldif` порядок и количество пробелов имеют важное значение.

2.3. Для применения внесенных изменений выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-enable-syncrepl-consumer.sh
```

2.4. Перезапустите сервис **OpenLDAP Service**:

```
sudo systemctl restart slapd
```

3. Настройте сервер-поставщик:

3.1. Ознакомьтесь с файлом `openldap-enable-syncrepl-provider.ldif`, устанавливаемым в составе SePlatform.Security:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la

dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpCheckpoint: 100 10
olcSpSessionlog: 100

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq
```

3.2. Замените **«{2}mdb»** на текущий тип БД, если он отличается, в строках:

- **«dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config»**;
- **«dn: olcDatabase={2}mdb,cn=config»**,

3.3. Для применения внесенных изменений выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-enable-syncrepl-provider.sh
```

3.4. Перезапустите сервис **OpenLDAP Service**:

```
sudo systemctl restart slapd
```

4. Настройте Агент SePlatform.Security:

4.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `/opt/SePlatform/SePlatform.Security`. Добавьте в секцию элемента `<LdapHosts>` строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

В данном примере:

- **«127.0.0.1»** - адрес локального сервера (поставщика);
- **«172.16.13.167»** - пример адреса сервера-приемника (укажите нужный адрес).

4.2. Перезапустите сервис:

```
sudo systemctl restart seplatform.security.service
```

3.3.1.2. Разнонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Убедитесь, что типы баз данных всех серверов - **«mdb»**, с помощью команды:

```
sudo slapcat -n0
```

Пример искомого значения: **«dn: olcDatabase={2}mdb,cn=config»**. Если база имеет тип, отличный от **«{2}mdb»**, во всех файлах, создаваемых и применяемых в инструкции ниже, следует указывать правильный тип базы.

2. Отключите все возможные репликации баз и серверов.
3. Убедитесь, что содержимое баз резервируемых серверов идентично.
4. Сделайте бэкап конфигурации с помощью команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/SePlatform/SePlatform.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

5. Остановите все программы, взаимодействующие с серверами OpenLDAP.
6. Убедитесь, что системное время резервируемых серверов одинаковое, иначе синхронизация изменений будет работать в одну сторону.
7. На время настройки резервирования одного из серверов остановите остальные резервируемые сервера OpenLDAP.

Чтобы настроить разнонаправленное резервирование:

1. На любом из резервируемых серверов создайте файл конфигурации `openldap-enable-syncrepl-multiprovider-server.ldif` со следующим содержанием:

```
###############################################################
# Check/modify database type (bdb/hdb/mbd/...), server ID (unique number),
# address of provider, binddn, credentials, searchbase.
###############################################################

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib64/openldap/
olcModuleLoad: syncprov.la

###############################################################

dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100

###############################################################

dn: cn=config
changetype: modify
replace: olcServerID
olcServerID: 1

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl:
  rid=001
  provider=ldap://192.168.56.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
olcSyncRepl:
  rid=002
  provider=ldap://192.168.57.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
```

```
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
-
add: olcMirrorMode
olcMirrorMode: TRUE

dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Обратите внимание, что отступ в каждой строке внутри конструкции olcSyncRepl обязательно должен содержать по два пробела.

2. Измените файл конфигурации следующим образом:

   2.1. В строке olcServerID: 1 придумайте и укажите идентификатор сервера;

   > ОБРАТИТЕ ВНИМАНИЕ
   > olcServerID должен быть уникальным для каждого резервируемого сервера.

   2.2. Замените **«{2}mdb»** на текущий тип БД, если он отличается, в строках:

   - **«dn: olcDatabase={2}mdb,cn=config»**;
   - **«dn: olcOverlay=syncprov,olcDatabase={2}mdb,cn=config»**

   2.3. Добавьте столько конструкций olcSyncRepl, сколько серверов участвуют в резервировании помимо текущего. Каждая конструкция olcSyncRepl описывает один из резервируемых серверов.

   > ОБРАТИТЕ ВНИМАНИЕ
   > Внутри одного сервера параметры rid разных конструкций olcSyncRepl должны иметь уникальные значения.

   2.4. В каждой конструкции olcSyncRepl укажите IP-адрес и порт сервера, который она описывает, в строке параметра provider.

3. Для применения внесенных изменений выполните команду:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f openldap-enable-syncrepl-
multiprovider-server.ldif
```

4. Перезапустите сервер:

```
sudo systemctl restart slapd
```

5. Повторите все описанные действия на каждом из резервируемых серверов.

6. Настройте Агент SePlatform.Security:

6.1. Перейдите к файлу конфигурации `seplatform.security.agent.xml`, расположенному в `/opt/SePlatform/SePlatform.Security`. Добавьте в секцию элемента `<LdapHosts>` строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
       <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

В данном примере:

- **«127.0.0.1»** - адрес локального сервера (поставщика);
- **«172.16.13.167»** - пример адреса сервера-приемника (укажите нужный адрес).

6.2. Перезапустите сервис:

```
sudo systemctl restart seplatform.security.service
```

После настройки последовательно включите все сервера OpenLDAP. Подключитесь напрямую к каждой базе и убедитесь, что ошибок не возникло. Для проверки внесите изменения в конфигурацию на одном из серверов. Убедитесь, что эти изменения появились и на других серверах.

4. Агент безопасности и его настройка

Агент безопасности представляет собой:

- службу **SePlatform.Security.Agent** на ОС Windows;
- сервис **seplatform.security.service** на ОС Linux.

Служба (сервис) выполняет следующие функции:

- Передает информацию между компонентами SePlatform.Security и программами, использующими сервис безопасности (например SePlatform.HMI.Alarms, SePlatform.HMI.Trends и пр.)
- Транслирует сообщения аудита безопасности в сигналы SePlatform.Data Server (стр. 82).
- Выполняет контроль целостности файлов и предоставляет сообщения о результатах с помощью компонентов SePlatform.HMI.Security.

Например, при регистрации пользователя в SePlatform.HMI.Alarms, введенные данные проверяются на LDAP-сервере агентом безопасности. Если данные верны, и пользователь имеет доступ к программе, агент безопасности запоминает пользователя как текущего, и передает сведения о правах пользователя из LDAP-сервера в SePlatform.HMI.Alarms.

После установки может понадобиться настройка агента безопасности. Для настройки Агент SePlatform.Security редактируйте конфигурационный файл `seplatform.security.agent.xml`, расположенный в:

- `C:\Program Files\SePlatform\SePlatform.Security` - для ОС Windows;
- `/opt/SePlatform/SePlatform.Security` - для ОС Linux.

После изменения настроек нужно перезапустить службу **SePlatform.Security.Agent**.

Пример настроенного конфигурационного файла находится в Приложение А: Пример конфигурационного файла Агент SePlatform.Security (стр. 101).

Настроить связь с узлами сети SePlatform.Net

Эта настройка необходима для установления связи между агентом безопасности и Net-агентом. Как правило агенты установлены на одном компьютере, и менять указанные здесь значения не требуется.

Чтобы установить связь SePlatform.Security с Net-агентом, в конфигурационном файле укажите адрес точки доступа SePlatform.Net.Agent в качестве значений атрибутов элемента `<EntryPointNetAgent>`:

- `Address` - IP-адрес Net-агента;
- `Port` - порт для подключения.

```
<EntryPointNetAgent Address="127.0.0.1" Port="1010"/>
```

Настроить связь с LDAP-сервером

Эта настройка выполняется в случае, если OpenLDAP и агент безопасности установлены на разных компьютерах.

Чтобы установить связь между Агент SePlatform.Security и LDAP-сервером, установленным на другом компьютере, укажите адрес и порт LDAP-сервера в качестве значений атрибутов элемента `<LdapHosts>`:

```
<LdapHosts>
       <LDAPServer Address="127.0.0.1" Port="389"/>
</LdapHosts>
```

Указать администратора LDAP

По умолчанию здесь указан логин стандартной учетной записи администратора LDAP.

- Для ОС Windows учетная запись создаётся автоматически. Логин - **«manager»**, пароль администратора - **«secret»**.
- Для ОС Linux учетная запись создаётся при установке OpenLDAP. Логин, указанный в конфигурационном файле по умолчанию - **«admin»**, пароль администратора задается при установке.

Если меняли администратора LDAP, укажите его логин в качестве значения атрибута `value` элемента `<LdapUser>` в указанном виде:

```
<LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>
```

ОБРАТИТЕ ВНИМАНИЕ

«dc=maxcrc,dc=com» - домен LDAP-сервера, указываемый для связи с Агент SePlatform.Security. Это значение менять нельзя.

«cn="логин-администратора",dc="домен-базы-данных"» - формат указания каталога, принятый для OpenLDAP.

Здесь же укажите пароль администратора в зашифрованном виде в качестве значения атрибута `value` элемента `<LdapPassword>`:

```
<LdapPassword value="VuZyuLC...JFchMHvKXNeztHoFpe24v2Wl9viv"/>
```

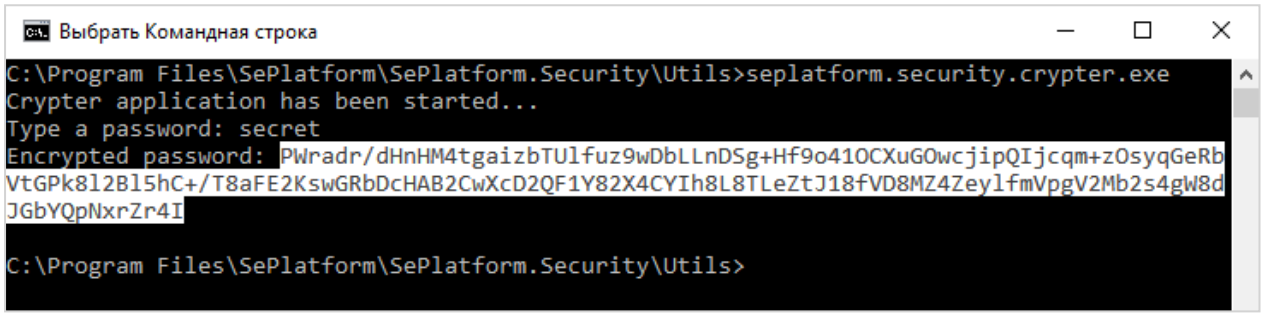
ПРИМЕЧАНИЕ

Когда необходимо зашифровать пароль, используйте приложение:

- `seplatform.security.crypter.exe`, расположенное в `C:\Program Files\SePlatform\SePlatform.Security\Utils` - для ОС Windows;
- `seplatform.security.crypter`, расположенное в `/opt/SePlatform/SePlatform.Security/Utils` - для ОС Linux.

Чтобы получить пароль в зашифрованном виде:

1. Запустите приложение через командную строку (терминал) от имени администратора.
2. Введите шифруемый пароль и нажмите **Enter**.
3. Зашифрованное значение скопируйте и вставьте в качестве значения атрибута `value` элемента `<LdapPassword>` в конфигурационный файл.



Пароли шифруются с использованием алгоритма Salted SHA-1 и хранятся в виде необратимых хэш-значений.

Указать пользователя по умолчанию

Можно указать пользователя по умолчанию - пользователя, чьи права используются, когда нет активной пользовательской сессии. Пользователем по умолчанию может быть любой пользователь из созданных при конфигурировании LDAP-сервера (стр. 61). В целях безопасности не указывайте пользователя, у которого есть права на редактирование конфигурации подсистемы безопасности.

Задайте имя пользователя в конфигурационном файле в качестве значения атрибута `value` элемента `<DefaultUser>`:

```
<DefaultUser value="ИМЯПОЛЬЗОВАТЕЛЯ"/>
```

Здесь же укажите пароль пользователя по умолчанию в зашифрованном виде в качестве значения атрибута `value` элемента `<DefaultUserPassword>`:

```
<DefaultUserPassword value="VuZyuLC...JFchMHvKXNeztHoFpe24v2Wl9viv"/>
```

Указать каталог LDAP для подключения

Этот параметр менять не нужно, если на LDAP-сервере всего один каталог, и вы создавали его с помощью мастера в SecurityConfigurator, как описано в 6.1. Подключение к LDAP-серверу из SecurityConfigurator (стр. 47), либо с помощью SePlatform.HMI.SecurityConfigurator.

Если же на LDAP-сервере хранится несколько разных каталогов (корневых папок), то по умолчанию нужно подключаться только к одному из них. Укажите название нужного каталога в качестве значения атрибута `value` элемента `<SecurityDn>`:

```
<SecurityDn value="ou=SePlatformSecurity,dc=maxcrc,dc=com"/>
```

где **«SePlatformSecurity»** - название каталога по умолчанию.

ОБРАТИТЕ ВНИМАНИЕ

«dc=maxcrc,dc=com» - домен LDAP-сервера, указываемый для связи с агентом безопасности. Это значение менять нельзя.

«ou="имя-каталога",dc="домен-базы-данных"» - формат указания каталога, принятый для OpenLDAP.

Изменить уровень логирования

Эта настройка реализована одним из атрибутов элемента `<Options>` в конфигурационном файле.

Чтобы изменить уровень логирования, назначьте атрибуту `LoggerLevel` значение:

- **«0»** - чтобы выводить в лог минимум информации о работе SePlatform.Security;
- **«2»** - чтобы выводить в лог всю необходимую информацию о работе SePlatform.Security;
- **«5»** - чтобы выводить в лог дополнительную информацию о работе SePlatform.Security.

ОБРАТИТЕ ВНИМАНИЕ

Рекомендуемое значение - **«2»**. Значение **«5»** следует использовать только при поиске и анализе ошибок.

Заблокировать использование горячих клавиш (только для ОС Windows)

Эта настройка реализована одним из атрибутов элемента `<Options>` в конфигурационном файле.

Чтобы запретить использование горячих клавиш, назначьте в качестве значения атрибута `kbDriverString` перечень сочетаний SCAN-кодов клавиш. SCAN-коды клавиш разделяются внутри сочетания символом **«+»**, а сами сочетания - символом **«;»**. Перечень SCAN-кодов можно посмотреть в Приложение B: SCAN-коды клавиш (стр. 103).

ПРИМЕР

```
kbDriverString="0x1D+0x38+0x53;0x1D+0x2A+0x01;"
```

Такое значение блокирует сочетания **«ctrl+alt+del»** и **«ctrl+shift+esc»**.

ОБРАТИТЕ ВНИМАНИЕ

Чтобы блокировка использования сочетаний клавиш выполнялась корректно, необходимо установить драйвер kbDriver, поставляемый вместе с дистрибутивом SePlatform.Security. Для этого перейдите к расположению `C:\Program Files\SePlatform\SePlatform.Security\kbDriver`. Инструкция по установке драйвера описана в расположенном здесь файле `readme_kbdriver_install.txt`.

Указать необходимость постоянного запроса значений прав с LDAP-сервера

Эта настройка реализована одним из атрибутов элемента `<Options>` в конфигурационном файле.

Значение атрибута `UseRightsCacheStorage` используется для выбора источника данных о правах:

- **«1»** - права пользователя не запрашиваются с LDAP-сервера, используются кэшированные значения прав;
- **«0»** - права пользователя запрашиваются с LDAP-сервера всегда.

Скрыть пользователя из запрашиваемого списка пользователей

Эта настройка реализована одним из атрибутов элемента `<Options>` в конфигурационном файле.

Значение атрибута `ReducedUserList` используется для сокращения списка пользователей, предоставляемого по запросу:

- **«1»** - по запросу предоставляется сокращенный список пользователей;
- **«0»** - по запросу предоставляется полный список пользователей.

Такой список предоставляется, например, в окне входа в конфигураторе. Чтобы исключить пользователя из полного списка, назначьте ему право **InteractiveLogon** с запрещающим значением. Подробнее право описано в Приложение D: Права стандартного приложения SePlatform.Security (стр. 109).

Транслировать сообщения из системного журнала в сообщения аудита безопасности (для ОС Linux)

Эта настройка реализована одним из атрибутов элемента `<Options>` в конфигурационном файле.

Значение атрибута `FAMode` позволяет настроить трансляцию выбранных сообщений из текстовых файлов (например, из системного журнала) в сигналы сообщений аудита (стр. 82):

- **«1»** - трансляция сообщений включена;
- **«0»** - трансляция сообщений отключена.

Чтобы выбрать сообщения для трансляции:

1. Перейдите к файлу `seplatform.security.fa.xml`, расположенному в `/opt/SePlatform/SePlatform.Security`.

2. Ознакомьтесь с содержанием файла. По умолчанию здесь описаны шаблоны сообщений, транслируемых из системных журналов `/var/log/auth.log` и `/var/log/secure`. Для каждого источника создан элемент `<FileRecords>` со вложенным элементом `<Records>`, внутри которого и описаны шаблоны сообщений - в элементах `<Rec>`. Назначение атрибутов элемента описано в этом же файле. Обратите внимание, что значения атрибута `EventType` соответствует названиям типов сообщений аудита - **«Normal»** или **«Admin»**. Эти названия можно менять - подробнее назначение типов описано в разделе 7. Аудит безопасности (стр. 82). Если типы были переименованы при настройке аудита, здесь эти значения тоже нужно изменить.

3. Раскомментируйте конструкции `<Rec>`, если необходимо транслировать описанные сообщения в аудит. Создайте собственные конструкции по аналогии, если необходимо транслировать сообщения иного вида.

5. Запуск сервисов (для ОС Linux)

Запуск сервиса seplatform.security.useractivity.service

Сервис предназначен для обслуживания сессий пользователя. Именно этот сервис позволяет отследить длительность сессии и время бездействия пользователя. Благодаря ему происходит автоматический выход пользователя из системы, если длительность сессии или время бездействия достигло установленного лимита.

По умолчанию сервис запускается автоматически. Чтобы посмотреть список запущенных сервисов, используйте команду `ps aux`. Для удобства поиска отфильтруйте результаты с помощью команды `grep`:

```
ps aux | grep seplatform.security
```

Если в списке не будет сервиса **`seplatform.security.useractivity.service`**, необходимо будет запустить его вручную.

Сервис запускается для каждого пользователя отдельно. Чтобы запустить сервис для конкретного пользователя, необходимо редактировать файл `seplatform.security.useractivity.sh`, расположенный в `/opt/SePlatform/SePlatform.Security`.

1. Откройте файл в текстовом редакторе, вызвав команду:

   ```
   sudo nano seplatform.security.useractivity.sh
   ```

   Значения, которые необходимо изменить, выделены цветом.

   ```
   #!/bin/sh
   # Установите правильный адрес дисплея для графического сервера в переменной окружения
   DISPLAY.
   # Пример: ":0".
   export DISPLAY=":0"
   # Установите правильный путь к файлу авторизации для графического сервера
   # (для того пользователя, от которого выполняется вход в графическую систему).
   # Пример: "/home/user1/.Xauthority".
   export XAUTHORITY="/home/user1/.Xauthority"
   # Укажите имя пользователя для запуска команды от его имени.
   sudo -u user1 /opt/SePlatform/SePlatform.Security/seplatform.security.useractivity
   ```

2. Здесь:

   - Укажите значение DISPLAY, зависящее от количества и конфигурации мониторов. Чтобы узнать значение, вызовите команду:

     ```
     export |grep DISPLAY
     ```

   - Вместо user1 укажите имя нужного пользователя.

3. Затем нажмите **`Ctrl`** + **`O`**, чтобы сохранить изменения, и **`Ctrl`** + **`X`**, чтобы выйти из редактора.

После этого стоит перезапустить систему. Проверьте список запущенных сервисов с помощью команды `ps aux`. Сервис **`seplatform.security.useractivity.service`** будет запущен от имени указанного пользователя.

Если же необходимо, чтобы сервис следил за сессией еще одного пользователя, необходимо добавить этого пользователя в конфигурацию сервиса. Для этого перейдите к файлу `seplatform.security.useractivity.add.anotheruser.sh`, расположенному в `/opt/SePlatform/SePlatform.Security`, и следуйте инструкции, описанной в нем.

Запуск сервисов агента безопасности от имени непривилегированного пользователя

Сервисы **`seplatform.security.service`** и **`seplatform.security.useractivity.service`**, как правило, запущены от имени суперпользователя root. Чтобы посмотреть, от чьего имени запущен сервис, используйте команду `ps aux`. Для удобства поиска отфильтруйте результаты с помощью команды `grep`:

```
ps aux | grep seplatform.security
```

Однако в некоторых случаях бывает необходимо разрешить запуск сервиса от имени непривилегированного пользователя. Для этого выполните следующие шаги:

1. Измените номер порта Net-агента на значение выше **«10000»** (например, **«11010»**). Это необходимо, потому что непривилегированным пользователям нельзя "прослушивать" порты с малыми номерами. Для этого:
   1.1. Перейдите к папке, где хранятся конфигурационные файлы агента безопасности - `/opt/SePlatform/SePlatform.Security`. Замените в конфигурационном файле `seplatform.security.agent.xml` номер порта Net-агента на новое значение.
   1.2. Затем перейдите к папке, где хранятся конфигурационные файлы SePlatform.Domain - `/opt/SePlatform/SePlatform.Domain`. Укажите новое значение порта в конфигурационных файлах `seplatform.net.agent.xml` и `seplatform.domain.agent.xml`.
2. Укажите имя непривилегированного пользователя в юнит-файлах:
   2.1. Перейдите к папке, содержащей юнит-файлы: `/lib/systemd/system/`.
   2.2. В файлах `seplatform.security.service`, `seplatform.security.useractivity.service`, `seplatform.security.service.backup` и `seplatform.security.useractivity.service.backup` замените значение root в строчках User=root и Group=root на имя непривилегированного пользователя, например User=test и Group=test.
3. Убедитесь в том, что непривилегированный пользователь имеет права на чтение и запись:
   - папки установки SePlatform.Security;
   - папок и файлов, для которых выполняется контроль целостности;
   - кэша конфигурации SePlatform.Domain.

После этого следует перезапустить систему. Проверьте список запущенных сервисов с помощью команды `ps aux`. Сервисы **`seplatform.security.service`** и **`seplatform.security.useractivity.service`** будут запущены от имени указанного пользователя.

6. Редактирование конфигурации на LDAP-сервере с помощью SecurityConfigurator

SecurityConfigurator - это программа для управления содержимым (конфигурирования) каталогов на LDAP-сервере. SecurityConfigurator позволяет:

- создавать учетные записи пользователей;
- объединять пользователей в группы для предоставления им одинаковых возможностей;
- создавать права доступа к приложениям и группировать права в приложения;
- создавать роли в приложениях и назначать их пользователям или группам;
- назначать права пользователям или группам;
- объединять АРМы, включенные в сеть SePlatform.Net, в кластерные рабочие места.

Просматривать и редактировать конфигурацию могут только администратор и пользователи, которым назначены разрешающие значения прав на просмотр и на редактирование конфигурации (стр. 71).

Чтобы запустить SecurityConfigurator, воспользуйтесь командой `Пуск → SePlatform → SecurityConfigurator`.

ПРИМЕЧАНИЕ

Можно запустить SecurityConfigurator с параметрами. Использование параметров при запуске позволяет управлять положением и внешним видом окна конфигуратора. Для запуска с параметрами используйте командную строку.

Возможные параметры запуска конфигуратора описаны в Приложение C: Параметры запуска SecurityConfigurator (стр. 107).

ОБРАТИТЕ ВНИМАНИЕ

SecurityConfigurator разработан только для ОС Windows. Если вы работаете на ОС Linux, можете использовать кроссплатформенный конфигуратор - SePlatform.HMI.SecurityConfigurator.

Однако, принцип конфигурирования подсистемы SePlatform.Security отличается в зависимости от используемого конфигуратора. Подробнее об этом будет написано в соответствующем подразделе.

ПРИМЕР

Раздел описывает создание и редактирование конфигурации на примере пробной конфигурации.

Предположим, все пользователи АРМ на предприятии делятся на две группы: диспетчеры и операторы. Диспетчеры могут управлять технологическим процессом, а операторы - наблюдать за технологическим процессом и передавать данные диспетчерам. Все они работают на одном участке. Кроме диспетчеров и операторов на участке работает начальник участка. Он может и наблюдать за технологическим процессом, и управлять им. Всем пользователям необходимо иметь возможность воспользоваться любым АРМ на предприятии.

Тогда, чтобы создать пробную конфигурацию, с помощью конфигуратора необходимо:

1. Создать три группы пользователей - **«Диспетчеры»**,**«Операторы»**, **«Начальники участков»**.
2. Создать приложение с правами на наблюдение и управление технологическим процессом и назначить их соответствующим группам пользователей.
3. Создать роль начальника участка в приложении.
4. Создать учетные записи пользователей и поместить их в группы, а также назначить роль начальнику.
5. Объединить в кластерное рабочее место все АРМ предприятия.

Чтобы приступить к созданию такой конфигурации, следует подключиться к LDAP-серверу и создать каталог.

6.1. Подключение к LDAP-серверу из SecurityConfigurator

SecurityConfigurator может подключаться к LDAP-серверу напрямую, либо с использованием Агент SePlatform.Security. При первом запуске SecurityConfigurator предложит подключиться к LDAP-серверу напрямую. Это необходимо для создания каталога на LDAP-сервере и учетной записи администратора SePlatform.Security.

ОБРАТИТЕ ВНИМАНИЕ

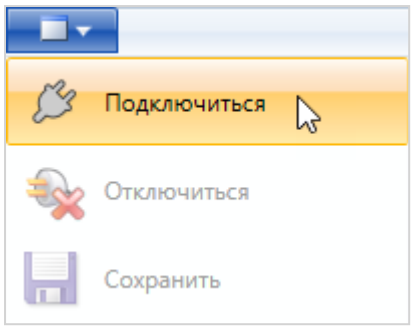
После первого подключения напрямую следует настроить подключение с помощью агента безопасности. Подключение напрямую к LDAP-серверу не позволяет пользоваться всеми возможностями SePlatform.Security. Только при подключении с помощью агента безопасности можно:

- пользоваться функцией аудита безопасности (стр. 82);
- использовать текущую пользовательскую сессию на разных АРМ, объединенных в кластерное рабочее место (стр. 75).

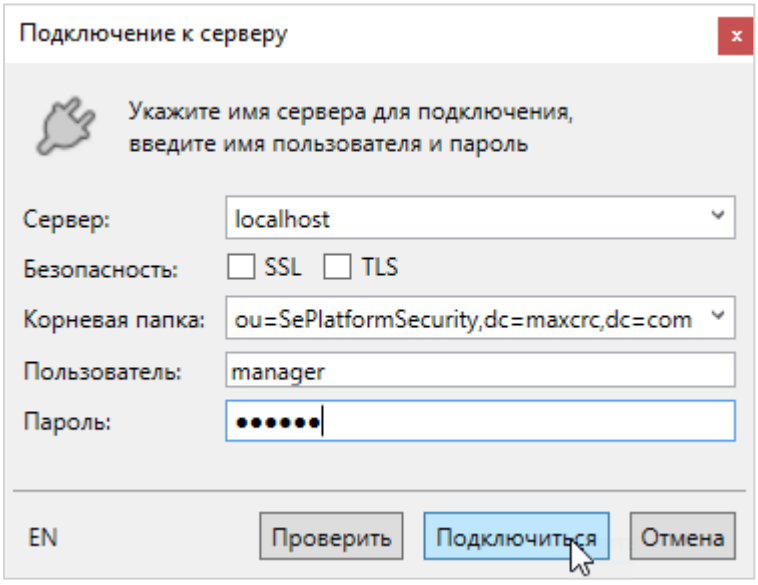
Подключение к LDAP-серверу напрямую

При подключении к LDAP-серверу напрямую:

1. В верхнем меню выберите **Подключиться...**.



2. В открывшемся окне **Подключение к серверу** укажите:
   - адрес LDAP-сервера (не меняйте, если OpenLDAP установлен на этом компьютере);
   - протокол безопасности (снимите галочки, если не собираетесь использовать протокол безопасности SSL или TLS при подключении. Подробнее об использовании протоколов безопасности - в Установка безопасного соединения с LDAP-сервером (стр. 51));
   - корневую папку:
     - если создаете новый каталог, можете указать любое название вместо стандартного **«SePlatformSecurity»**;
     - если подключаетесь к конкретному каталогу, укажите его имя, указанное при настройке Агент SePlatform.Security;
   - логин администратора безопасности (при первом подключении можно указать любой: здесь создается учетная запись администратора SePlatform.Security);
   - пароль администратора безопасности (при первом подключении можно указать любой).



3. Нажмите кнопку **Проверить** или **Подключиться**. SecurityConfigurator проверит, существует ли каталог (корневая папка) с указанным именем на LDAP-сервере. Если не существует, запустится **Мастер создания новой конфигурации**, который предложит создать каталог с указанным именем. В окне мастера:

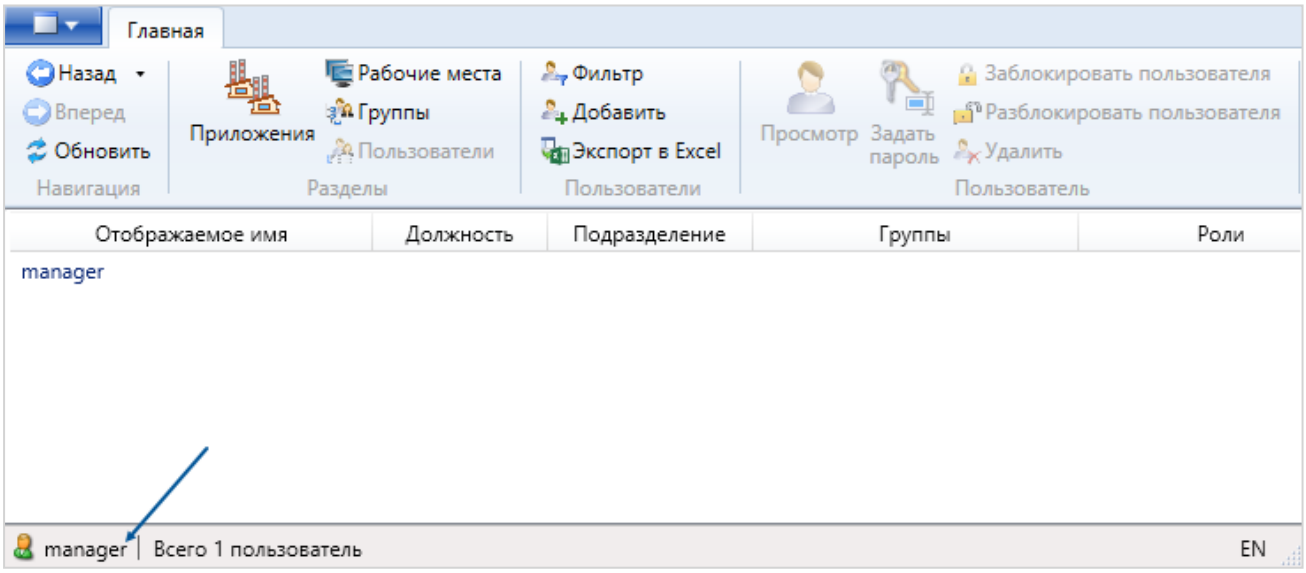
- На вкладке **LDAP** заполните поля:
  - **Администратор LDAP** в формате cn=ИМЯ-АДМИНИСТРАТОРА,dc=ДОМЕН-БАЗЫ-ДАННЫХ (**«manager»** - если OpenLDAP установлен на Windows, **«admin»** - если на Linux);
  - **Пароль администратора LDAP** (**«secret»** по умолчанию).
- На вкладке **Администратор** заполните поля:
  - **Администратор безопасности** (логин администратора SePlatform.Security, указанный при первом подключении);
  - **Пароль администратора** (пароль администратора SePlatform.Security, указанный при первом подключении).

В результате будут созданы:

- каталог на LDAP-сервере;
- учетная запись администратора SePlatform.Security с правами на просмотр и редактирование созданного каталога.

> ПРИМЕЧАНИЕ
>
> В дальнейшем новые каталоги создаются так же: при подключении к LDAP-серверу из SecurityConfigurator введите нужное имя нового каталога в поле **Корневая папка** и нажмите **Проверить** или **Подключиться**.

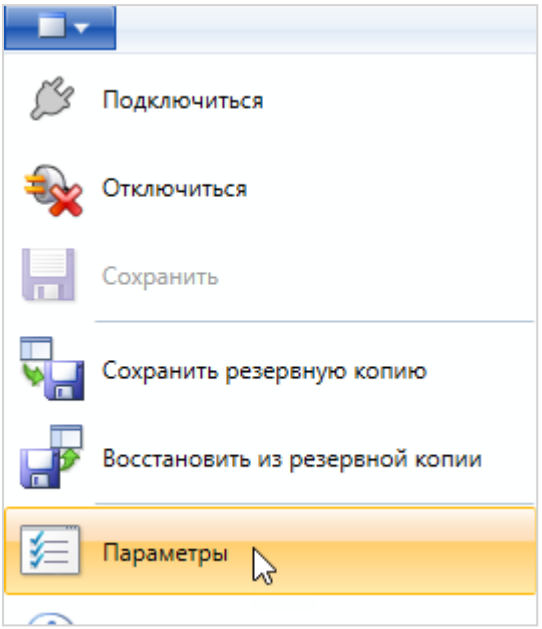
4. После подключения к указанному каталогу станет доступно редактирование его конфигурации от имени созданного администратора.



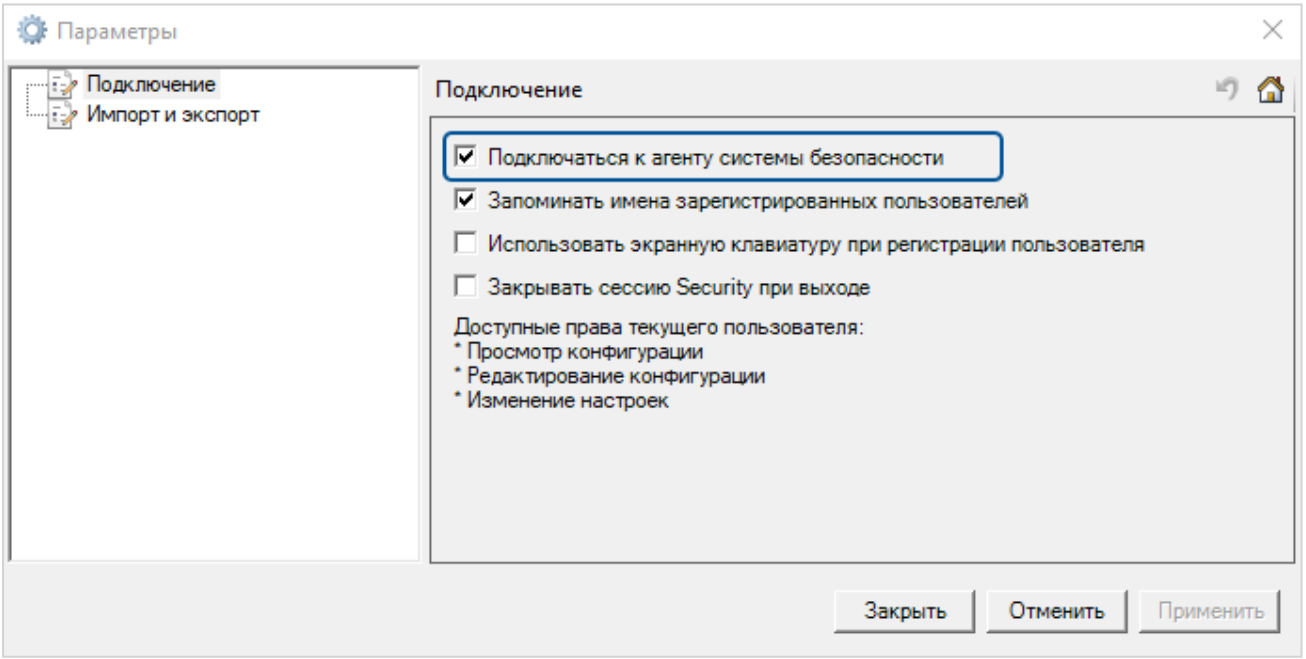
Подключение к LDAP-серверу с помощью агента безопасности

Чтобы настроить подключение к LDAP-серверу с помощью агента безопасности:

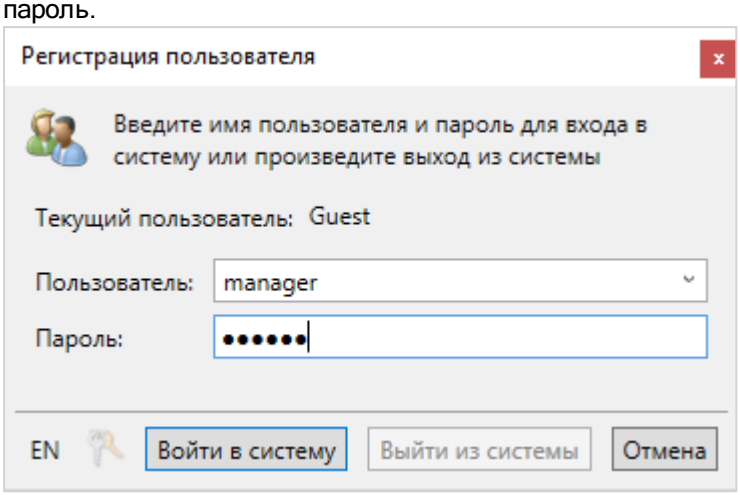
1. В верхнем меню выберите **Параметры**.



2. В открывшемся окне на вкладке **Подключение** установите галочку в пункте **Подключаться к агенту системы безопасности**.



Теперь при подключении к текущему каталогу достаточно будет вводить только логин администратора и пароль.



В таком случае при наличии активной пользовательской сессии ввод пароля при запуске конфигуратора можно сделать необязательным. Для этого необходимо изменить конфигурационный файл `defaultPassReq.xml`, расположенный в `C:\ProgramData\SePlatform\SePlatform.SecurityConfigurator`. Ознакомьтесь с этим файлом:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration ProductName="SePlatform.SecurityConfigurator" ProductVersion="">
 <Configurable Id="defaultPassReq">
  <DefaultPasswordRequirementsSettings>
   <DigitsRequired>true</DigitsRequired>
   <UpperRequired>false</UpperRequired>
   <LowerRequired>false</LowerRequired>
   <SpecialRequired>false</SpecialRequired>
   <MinimalPasswordLength>7</MinimalPasswordLength>
   <MinimalPasswordHistoryLength>4</MinimalPasswordHistoryLength>
   <IdentityConfirmation>true</IdentityConfirmation>
  </DefaultPasswordRequirementsSettings>
 </Configurable>
</Configuration>
```

Параметр, регулирующий необходимость подтверждения личности - элемент `<IdentityConfirmation>`. Измените значение по умолчанию **«true»** на **«false»**, чтобы при наличии активной пользовательской сессии при запуске конфигуратора не требовалось вводить пароль для подтверждения личности.

Подробнее назначение файла и остальных элементов описано в подразделе Изменить начальные значения прав на уровне приложения (стр. 66).

Установка безопасного соединения с LDAP-сервером

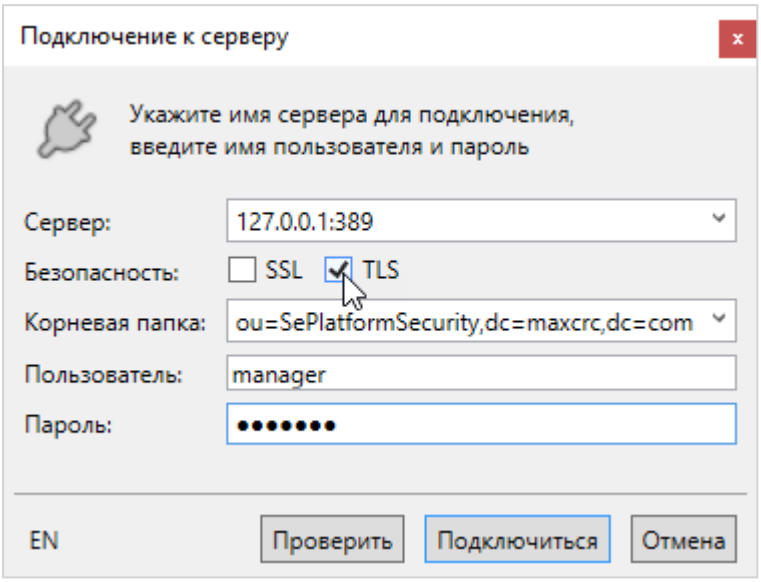
Для защиты соединения при подключении к LDAP-серверу можно выбрать один из протоколов безопасности: SSL или TLS[1]. Для использования протокола необходимо установить сертификат.

[1]SSL и TLS - криптографические протоколы, шифрующие передаваемые данные. После того, как протокол SSL был стандартизирован IETF (Internet Engineering Task Force), он был переименован в TLS. Поэтому SSL и TLS отличаются только номером описываемой версии одного и того же протокола.

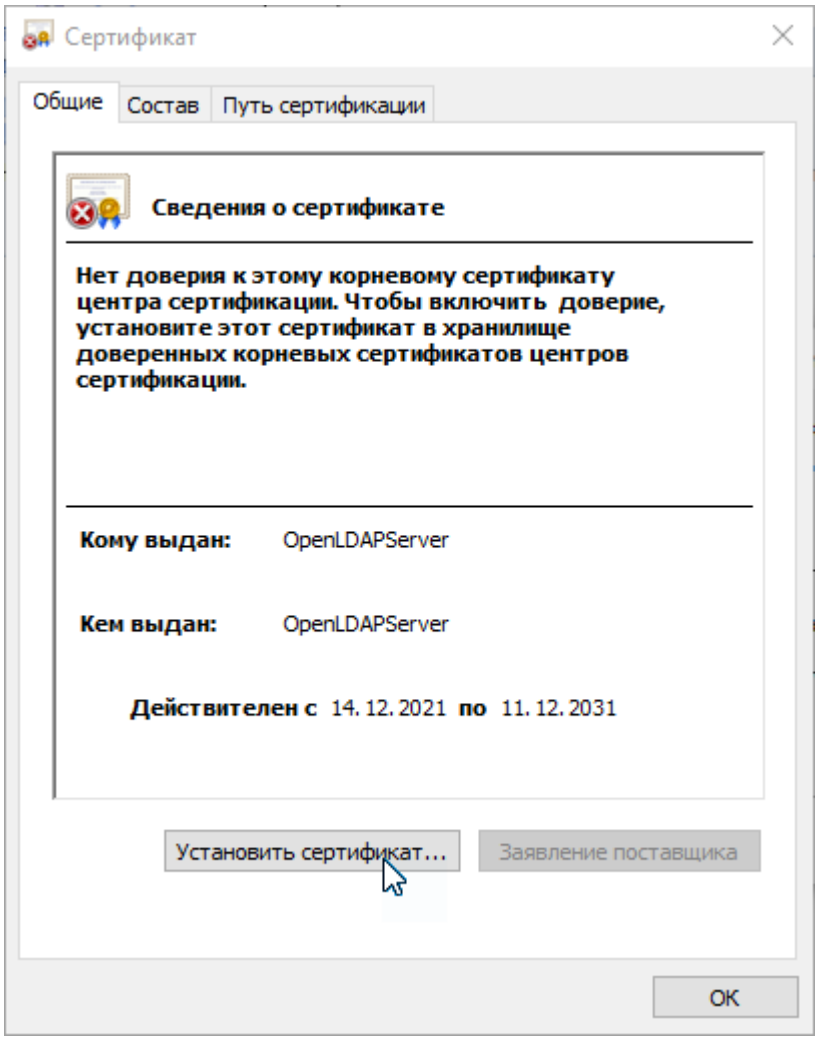
Сертификаты протоколов поставляются вместе с дистрибутивом SePlatform.Security. Сертификат достаточно установить один раз.

Сертификат устанавливается следующим образом:

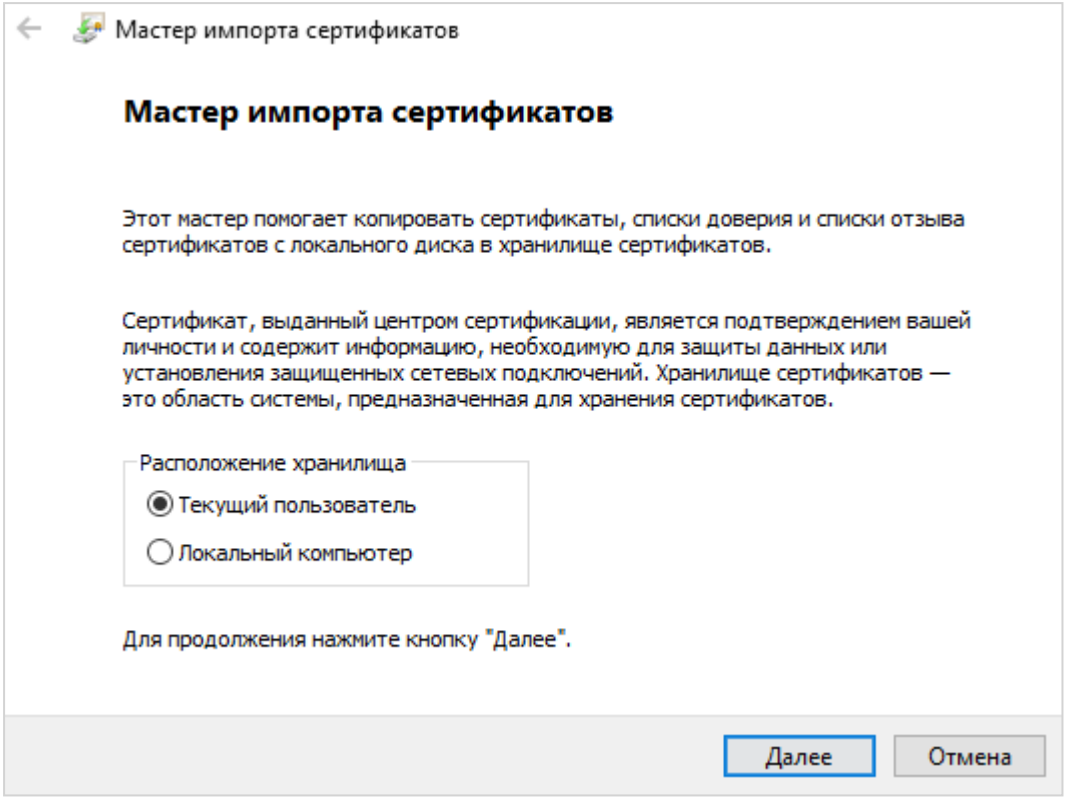
1. При подключении к LDAP-серверу напрямую из SecurityConfigurator в окне **Подключение к серверу** галочкой отметьте название протокола, который хотите использовать. Нажмите **Подключиться**.



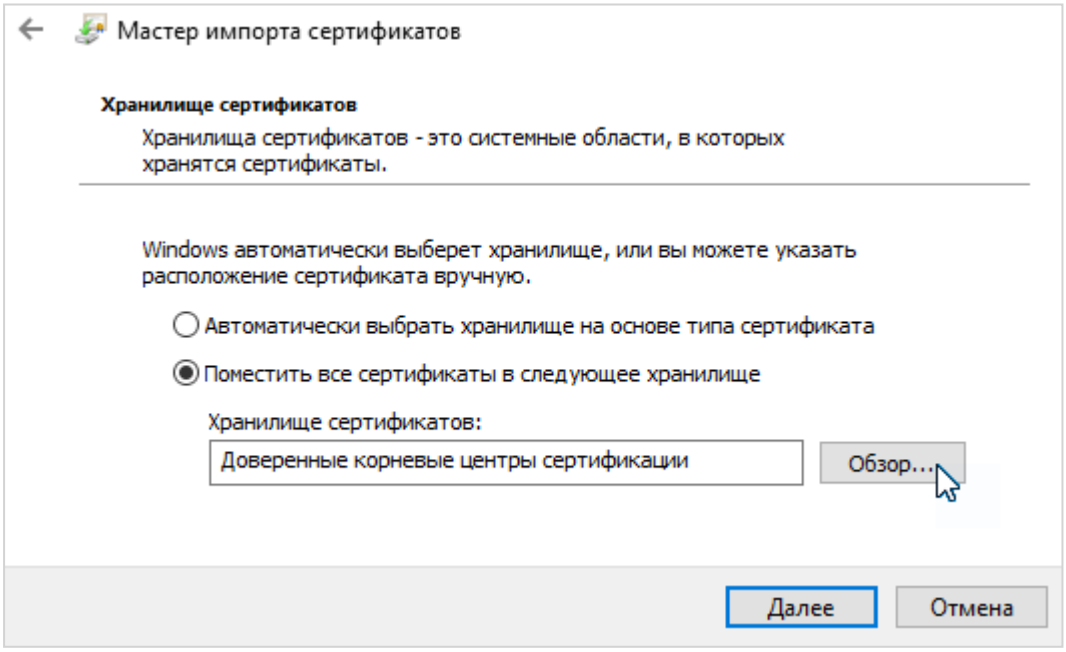
2. Операционная система предложит установить сертификат. Нажмите **Установить сертификат...**.



3. В открывшемся окне **Мастер импорта сертификатов** в области **Расположение сертификата** выберите **Текущий пользователь** и нажмите кнопку **Далее**.



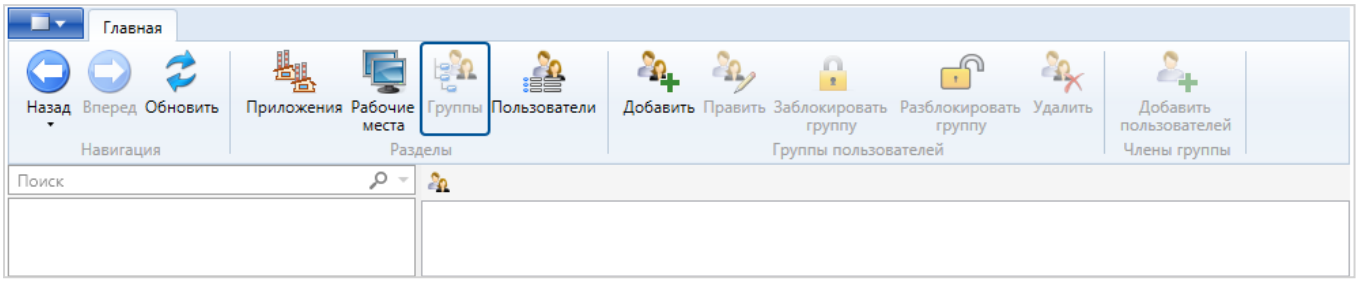
4. На следующем шаге выберите **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор...**. В открывшемся окне **Выбор хранилища сертификата** выберите папку Доверенные корневые центры сертификации и нажмите **ОК**. Диалоговое окно закроется.



5. В окне мастера нажмите **Далее**, а затем - **Готово**. Подтвердите импорт сертификата в открывшемся диалоговом окне. В конце концов, в окне мастера появится сообщение **Импорт успешно выполнен**.

6.2. Создание и редактирование групп пользователей

Чтобы приступить к работе с группами пользователей, перейдите в раздел **Группы**.



В разделе **Группы** можно:

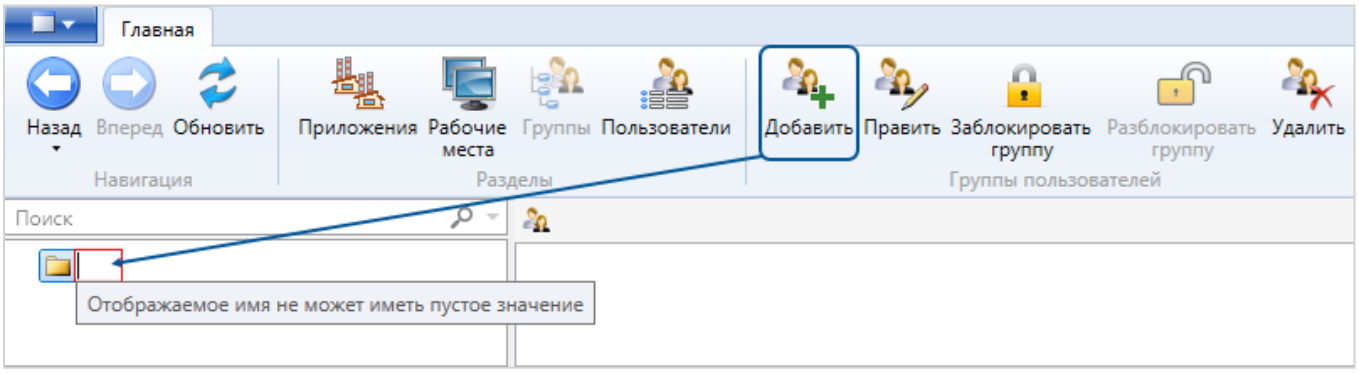
- создавать и удалять группы;
- блокировать и разблокировать группы;
- добавлять пользователей в группы;
- переходить к редактированию групп.

ПРИМЕР

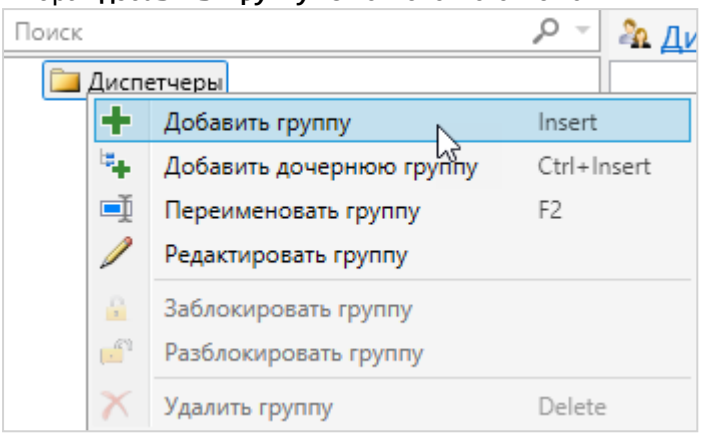
Для пробной конфигурации создайте группы **«Диспетчеры»**, **«Операторы»** и **«Начальники участка»**.

Создать группу

В разделе **Группы** нажмите **Добавить** на панели инструментов. В создавшемся поле введите название группы.



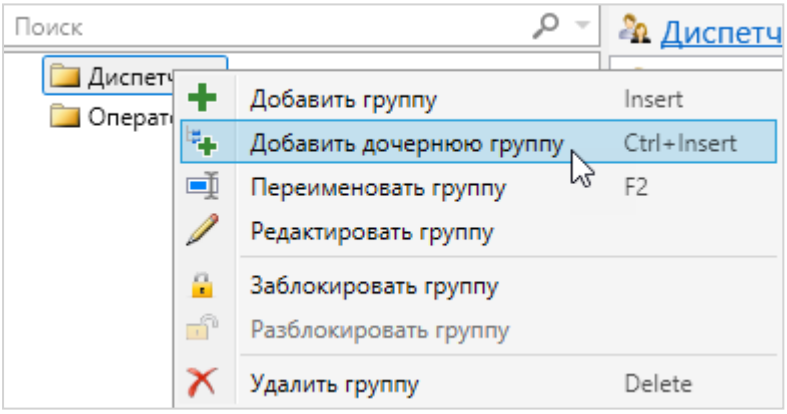
Если в списке уже есть хотя бы одна группа, новую группу можно создать, нажав ПКМ в списке групп и выбрав **Добавить группу** из контекстного меню.



Создать дочернюю группу

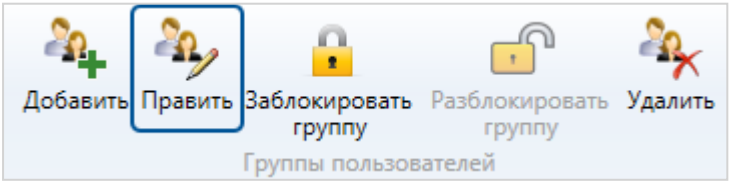
В группы можно добавлять дочерние группы. Дочерние группы можно использовать, например, когда необходимо наследовать права родительской группы.

Выберите в списке группу, в которую нужно добавить дочернюю группу, и выберите соответствующий пункт в контекстном меню по щелчку ПКМ.

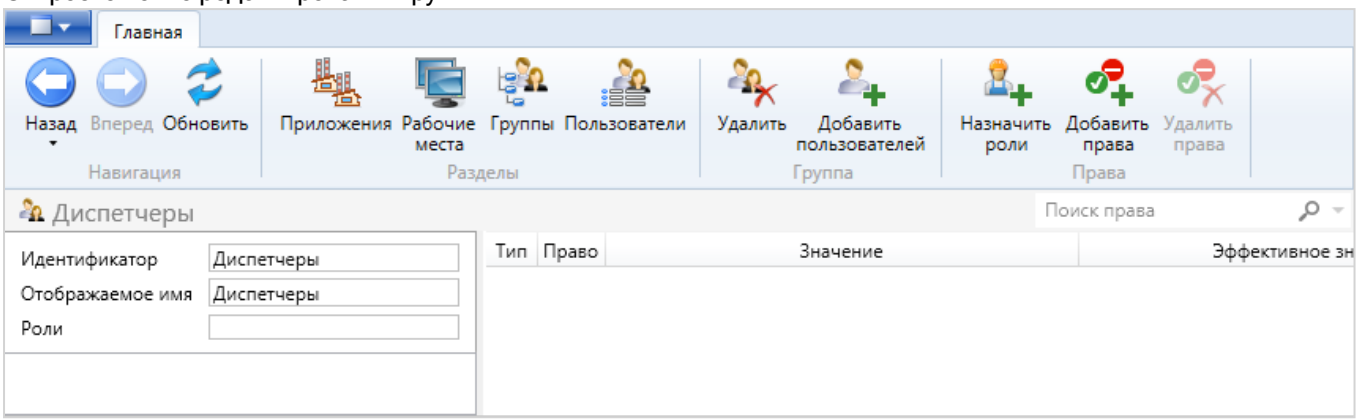


Редактировать группу

В разделе **Группы** выберите группу в списке и нажмите **Править** на панели инструментов, либо **Редактировать группу** в контекстном меню по щелчку ПКМ.



Откроется окно редактирования группы.



В окне редактирования группы можно:

- изменить идентификатор группы на LDAP-сервере, изменив значение поля **Идентификатор**;
- изменить отображаемое название группы, изменив значение поля **Отображаемое имя**;
- добавить в группу пользователей и удалить пользователей из группы;
- назначить группе роль и лишить роли;
- назначить группе права и лишить прав;
- удалить группу.

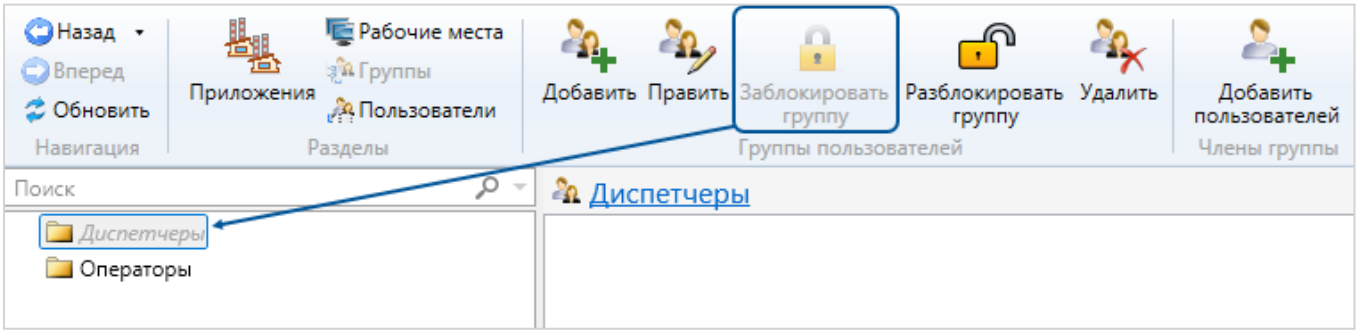
ПРИМЕЧАНИЕ

Чтобы выбрать несколько пользователей при добавлении в группу, используйте комбинацию клавиш «**Ctrl**» + «**Shift**».

Заблокировать группу

Группы можно блокировать. Блокируйте группы, когда необходимо ограничить доступ участников к АРМ. Пока участник группы заблокирован, его попытки входа отклоняются подсистемой безопасности.

Чтобы заблокировать группу, выберите группу в списке и нажмите **Заблокировать группу**, либо **Заблокировать группу** в контекстном меню по щелчку ПКМ. Заблокированные группы выделяются в списке серым цветом и курсивом.



Учетные записи пользователей, состоящих в заблокированной группе, в списке пользователей выделяются серым цветом и жирным шрифтом.

6.3. Создание и редактирование прав и приложений

Возможности пользователей в проекте определяются наличием у них разрешений и запретов на определенные действия. Информация о том, разрешено или запрещено пользователю какое-либо действие, хранится виде значения права. Права следует создавать внутри приложений. Приложения позволяют группировать права по какому-либо признаку и создавать роли (стр. 60), которые впоследствии можно назначать пользователям и группам.

При создании права нужно определить его тип.

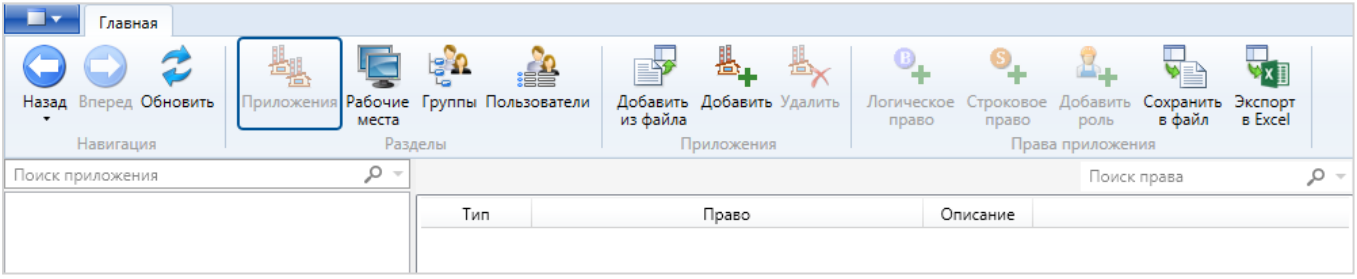
- Логическое право может иметь одно из двух значений: **«разрешено»** или **«запрещено»**.

  Применяется, когда необходимо разрешать или запрещать какие-либо действия пользователей в проекте. Например, одному пользователю разрешено печать отчеты (значение права - **«true»**), а другому - запрещено (значение права - **«false»**).

- Строковое право в качестве значений предоставляет строки. Одна строка - разрешенное значение, вторая - запрещенное значение.

  Применяется, когда необходимо получить список возможностей пользователя в текстовом виде. Например, списки отчетов, которые пользователь может и не может печатать.

Чтобы приступить к работе с правами и приложениями, перейдите в раздел **Приложения**.



В разделе приложений можно:

- создавать и удалять приложения;
- импортировать приложения из файла и экспортировать в файл;
- добавлять в приложения права и удалять права из приложений;
- редактировать права;
- создавать и удалять роли в приложениях.

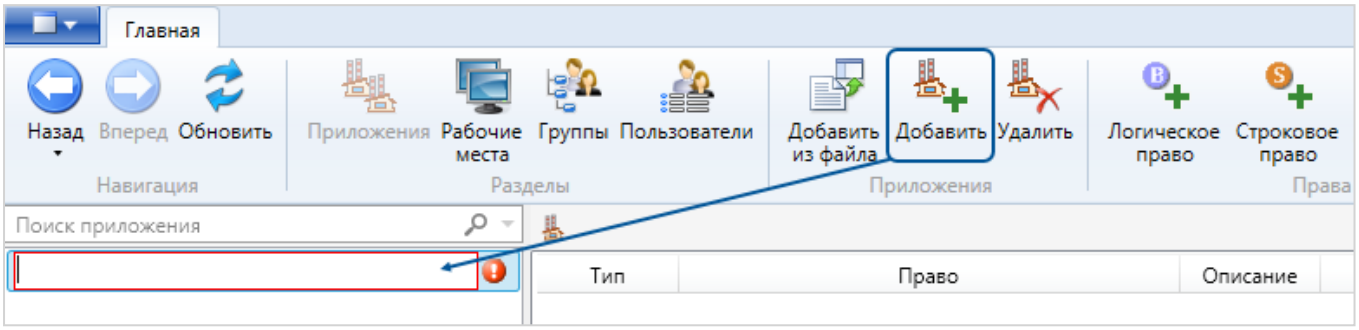
ПРИМЕР

Для пробной конфигурации создайте приложение **«Участок 1»**, содержащее права пользователей, работающих на одном участке:

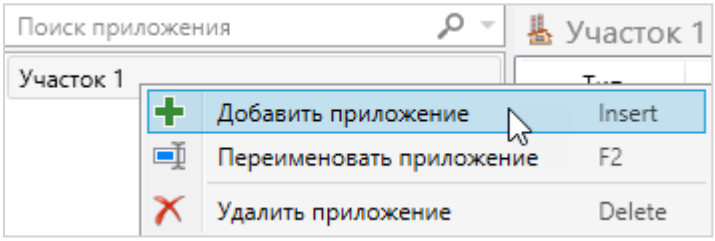
- одно логическое право для доступа к просмотру состояния технологического процесса;
- одно логическое право для доступа к управлению технологическим процессом.

Создать приложение

В разделе приложений нажмите **Добавить** на панели инструментов. В создавшемся поле введите название приложения.

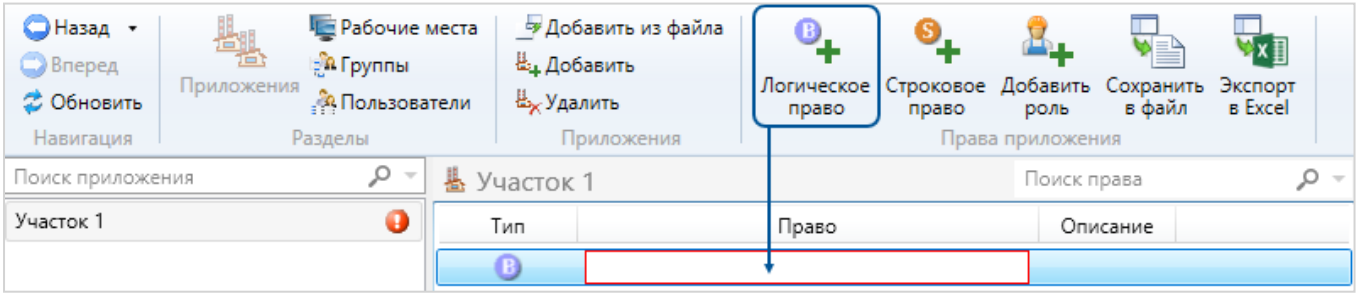


Если в списке уже есть хотя бы одно приложение, новое приложение можно создать, нажав ПКМ в списке приложений и выбрав **Добавить приложение** из контекстного меню.



Добавить право в приложение

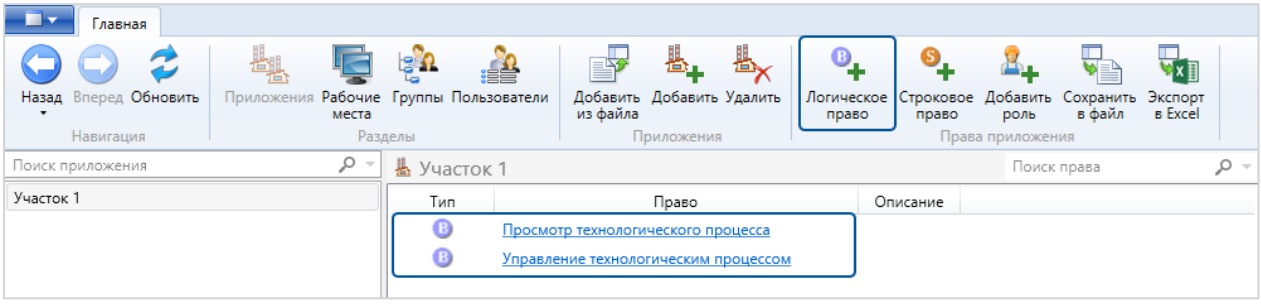
Чтобы добавить в приложение право, нажмите **Логическое право** или **Строковое право** на панели инструментов в зависимости от того, право какого типа нужно создать. В создавшемся поле введите название права.



ПРИМЕР

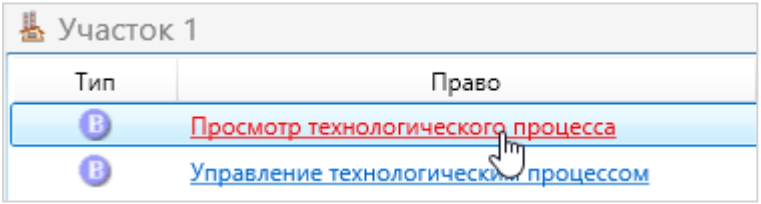
Добавьте в приложение **«Участок 1»** два логических права:

- **«Просмотр технологического процесса»** - разрешает или запрещает просмотр состояния технологического процесса;
- **«Управление технологическим процессом»** - разрешает или запрещает управление технологическим процессом.

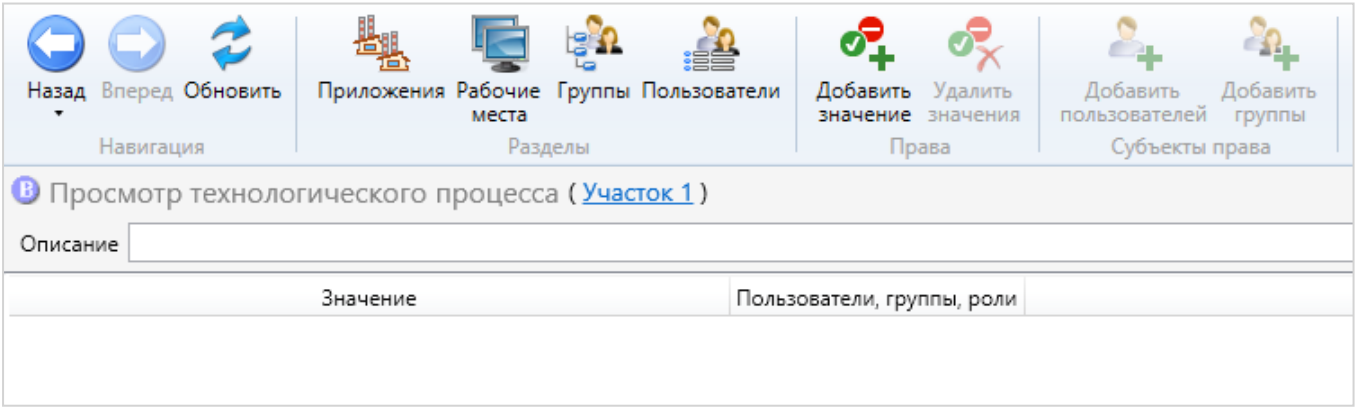


Редактировать право

Щелкните на название права в списке.



Откроется окно редактирования права.



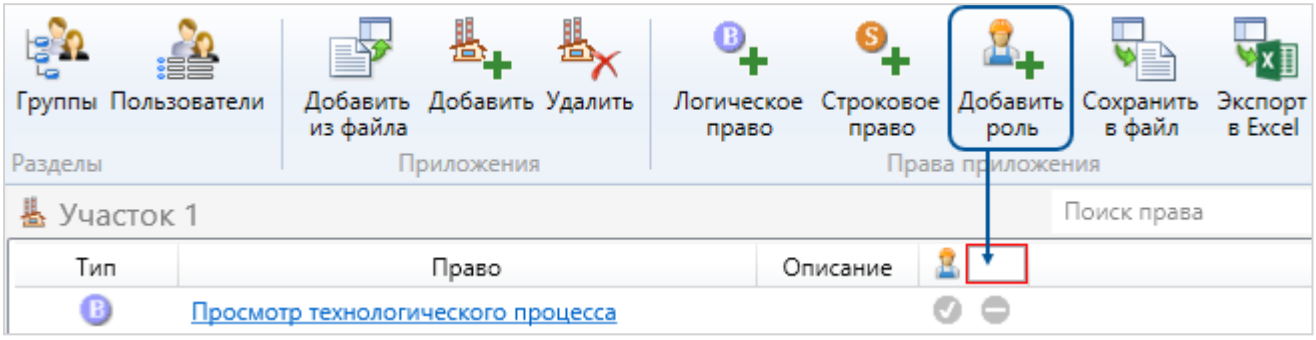
В окне редактирования права можно:

- редактировать описание права, изменив значение поля **Описание**;
- добавлять и удалять значения права;
- назначать значения прав группам и пользователям.

6.4. Создание ролей

Внутри приложения можно создать роль. Роль - это совокупность значений каждого права приложения. Роль может быть назначена как пользователю, так и группе.

Создание и редактирование ролей ведется в разделе приложений. Чтобы создать роль, выберите приложение из списка и нажмите **Добавить роль**. В создавшемся поле введите название роли.



Укажите значения прав для созданной роли:

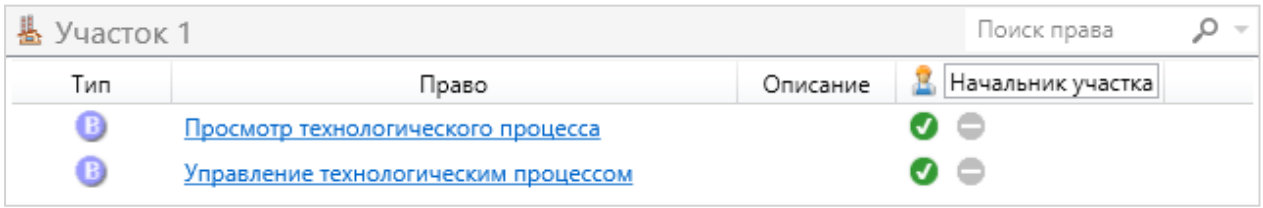
- - разрешающее значение логического права;
- - запрещающее значение логического права;
- текст 1 - разрешающее значение строкового права;
- текст 2 - запрещающее значение строкового права;

либо оставьте значение неопределенным:

- - для логического права;
- - для строкового права.

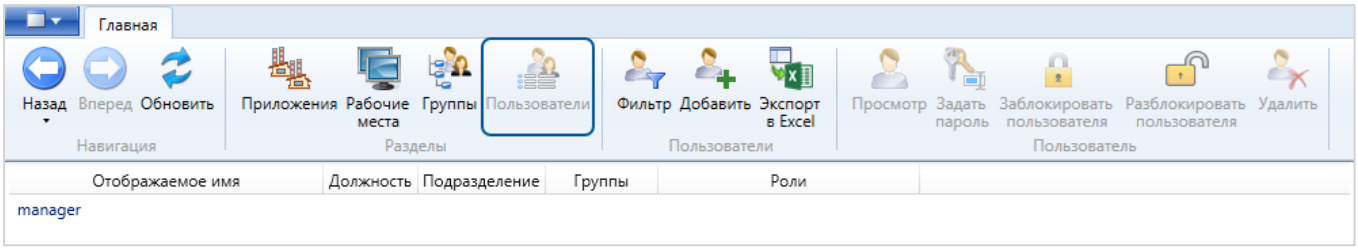
ПРИМЕР

Создайте роль начальника участка, имеющего разрешения на просмотр и управление технологическим процессом.



6.5. Создание и редактирование учетных записей

Чтобы приступить к работе с учетными записями пользователей, перейдите в раздел **Пользователи**.



В разделе **Пользователи** можно:

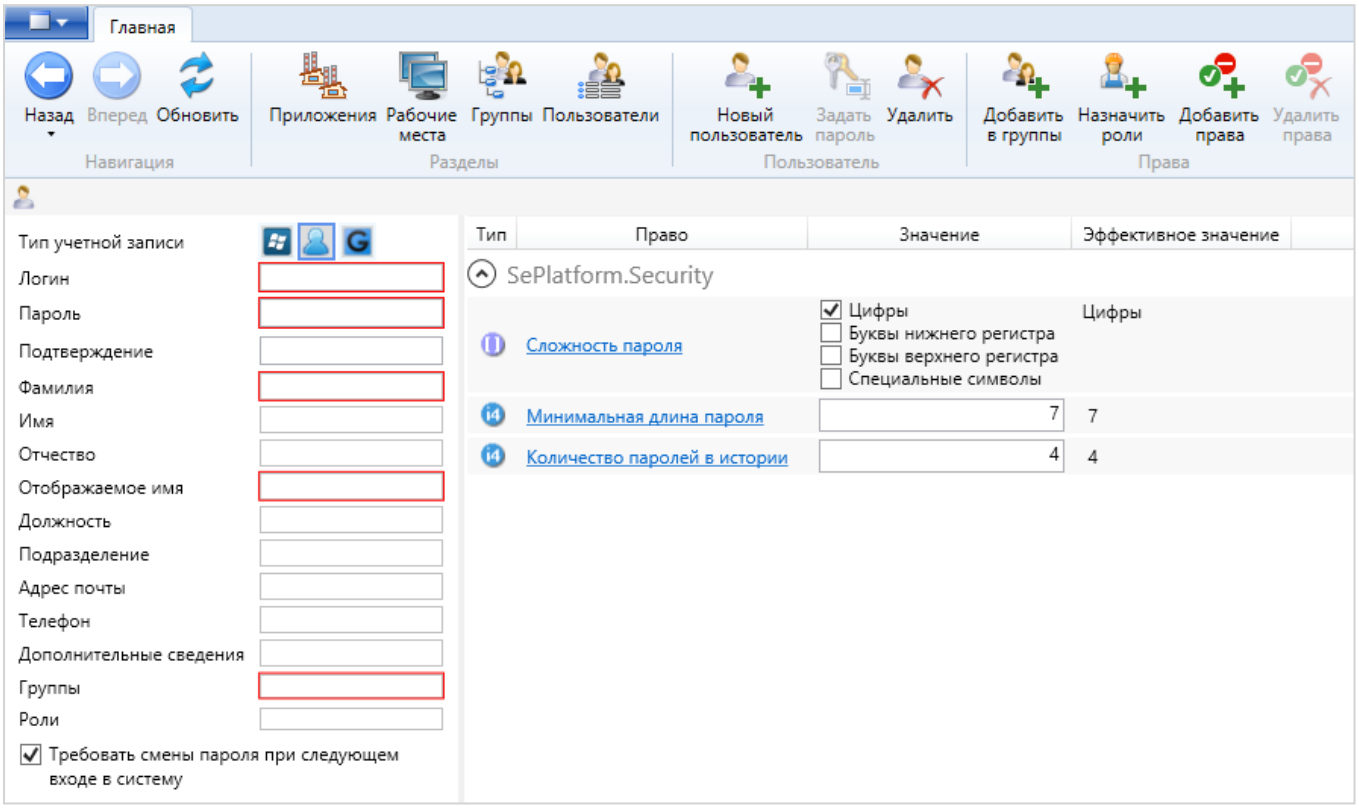
- создавать и удалять учетные записи пользователей;
- блокировать и разблокировать пользователей;
- принудительно менять пароли учетных записей;
- экспортировать список учетных записей в файл.

ПРИМЕР

Для пробной конфигурации создайте трех пользователей - диспетчера, оператора и начальника участка. При создании поместите пользователей в соответствующие группы. Начальнику участка, помимо группы, назначьте роль **«Начальник участка»**.

Создать учетную запись

В разделе **Пользователи** нажмите **Добавить** на панели инструментов. Откроется окно создания и редактирования учетной записи.



Новая учетная запись может быть одного из трех типов:

- учетная запись из Active Directory или ОС Windows ;
- локальная учетная запись SePlatform.Security ;
- учетная запись сервера безопасности Iconics .

Выберите нужный тип учетной записи, переключая иконки.

ПРИМЕЧАНИЕ

Для пробной конфигурации создавайте локальные записи SePlatform.Security.

Создать локальную учетную запись SePlatform.Security

Заполните обязательные поля:

- логин;
- пароль;
- фамилия;
- отображаемое имя (заполняется автоматически и состоит из фамилии, имени и отчества; полученное значение можно менять);
- группа.

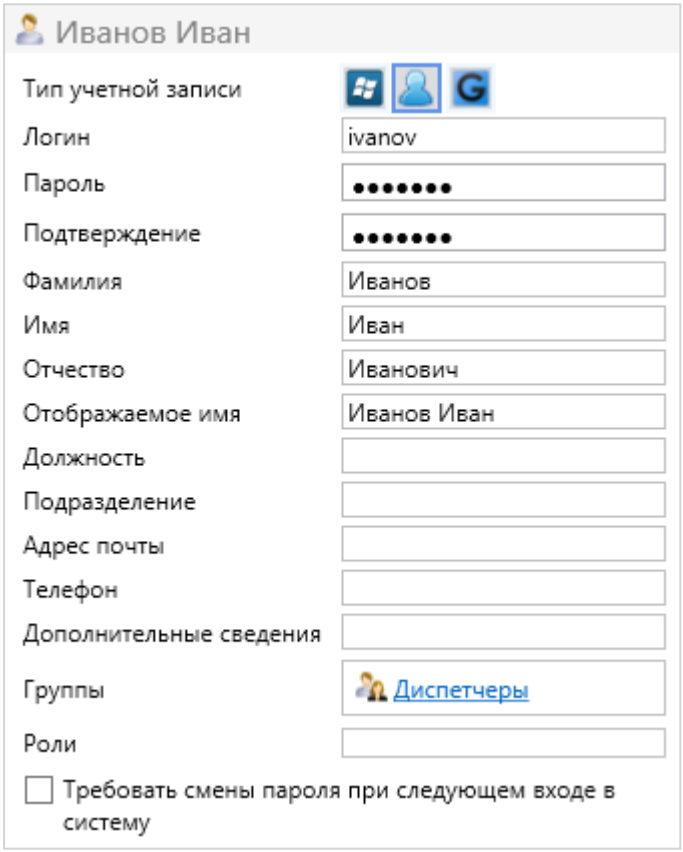
ПРИМЕЧАНИЕ

Для защиты паролей создаваемых учетных записей используется алгоритм криптографического хеширования. Полученное хеш-значение является необратимым. Для повышения криптографической стойкости используется "присаливание" - добавление к паролю неизвестной последовательности данных перед шифрованием. Это делается для предотвращения декодирования полученного хеш-значения.

ПРИМЕР

Для пробной конфигурации создайте трех пользователей и добавьте в группы, например:

- **«Иванов Иван»** - в группу **«Диспетчеры»**;
- **«Петров Петр»** - в группу **«Операторы»**;
- **«Семенов Семен»** - в группу **«Начальники участка»**, а также назначьте роль **«Начальник участка»**.



ОБРАТИТЕ ВНИМАНИЕ

Пользователя обязательно добавлять в группу. При этом пользователь может состоять только в одной группе.

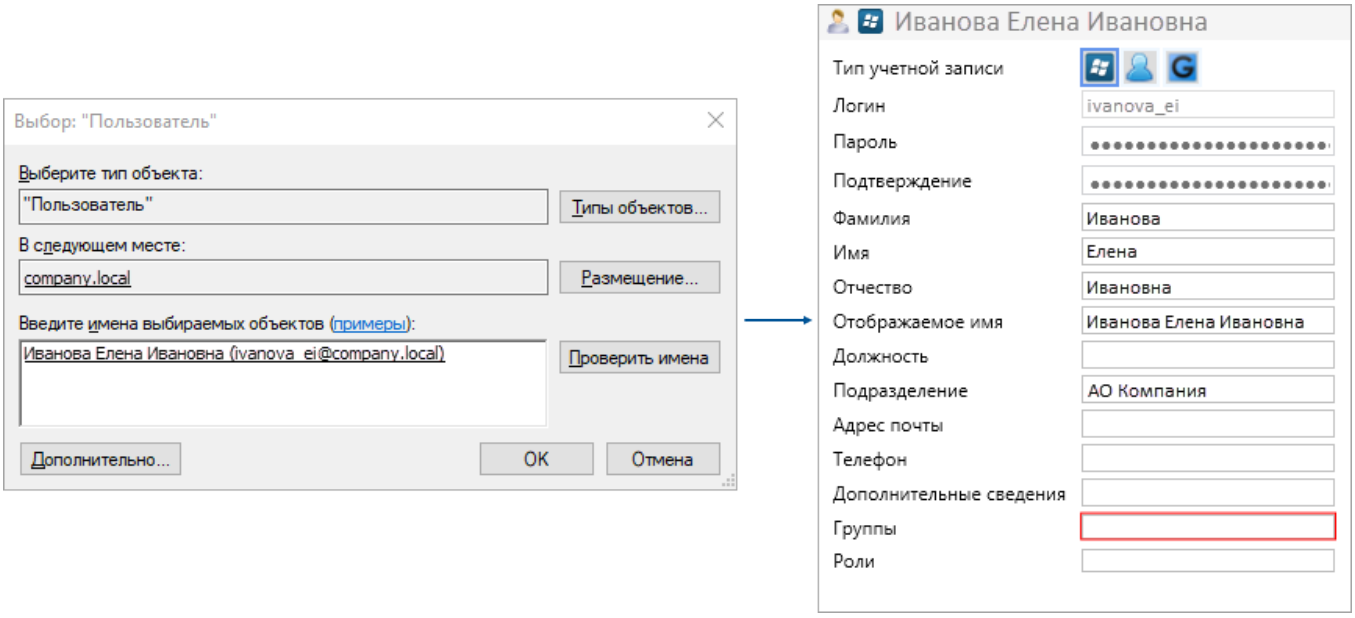
Создать учетную запись из ОС или Iconics

Если выбрать учетную запись из ОС Windows или Iconics, все нужные данные пользователя, кроме группы, будут подставлены в поля автоматически.

ПРИМЕЧАНИЕ

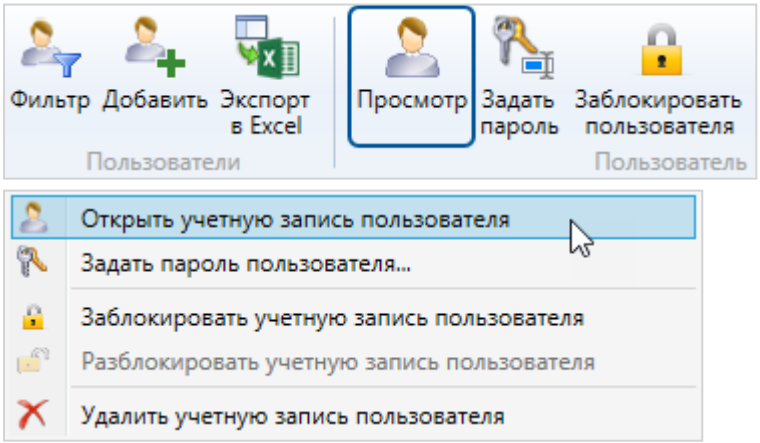
Прежде чем сохранить учетную запись, добавьте пользователя в группу.

Например, в результате нажатия откроется окно выбора пользователя из числа пользователей ОС.



Редактировать учетную запись

В разделе **Пользователи** выберите пользователя в списке и нажмите **Просмотр** на панели инструментов, либо **Открыть учетную запись пользователя** в контекстном меню по щелчку ПКМ.



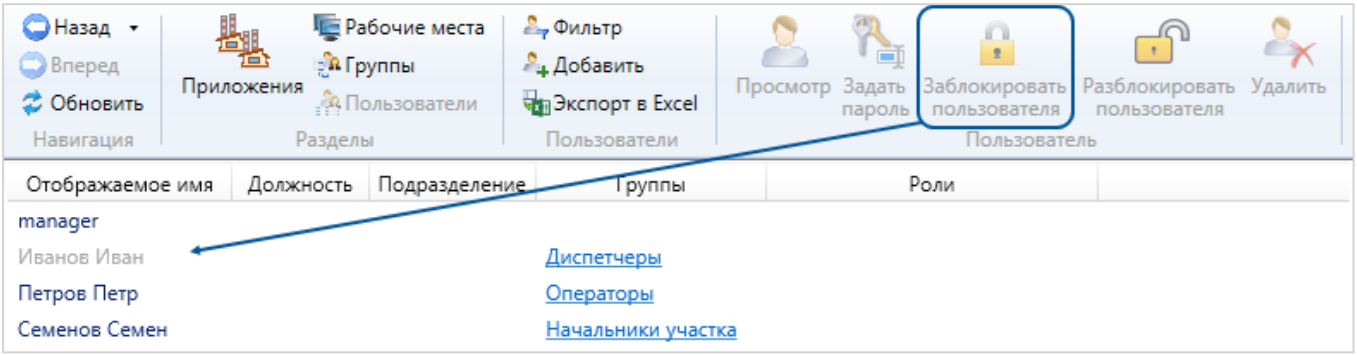
Откроется окно редактирования учетной записи пользователя. В окне редактирования учетной записи можно:

- менять сведения о пользователе (логин, фамилия, имя, телефон и пр.), изменяя значения соответствующих полей;
- изменить пароль пользователя, используя кнопку **Задать пароль** на панели инструментов;
- добавить пользователя в группу и удалить пользователя из группы;
- назначить пользователю роль и лишить роли;
- назначить пользователю права и лишить прав;
- удалить учетную запись пользователя.

Заблокировать пользователя

Пользователей можно заблокировать. Блокируйте пользователей, когда необходимо ограничить их доступ к АРМ. Пока пользователь заблокирован, его попытки входа отклоняются подсистемой безопасности.

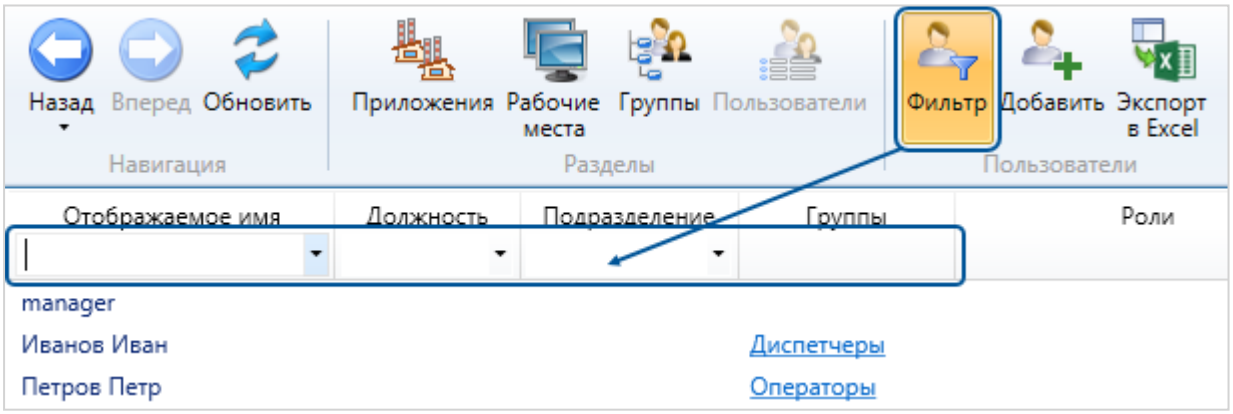
Чтобы заблокировать пользователя, выберите пользователя в списке и нажмите **Заблокировать пользователя**, либо **Заблокировать учетную запись пользователя** в контекстном меню по щелчку ПКМ. Учетные записи заблокированных пользователей выделяются в списке серым цветом.



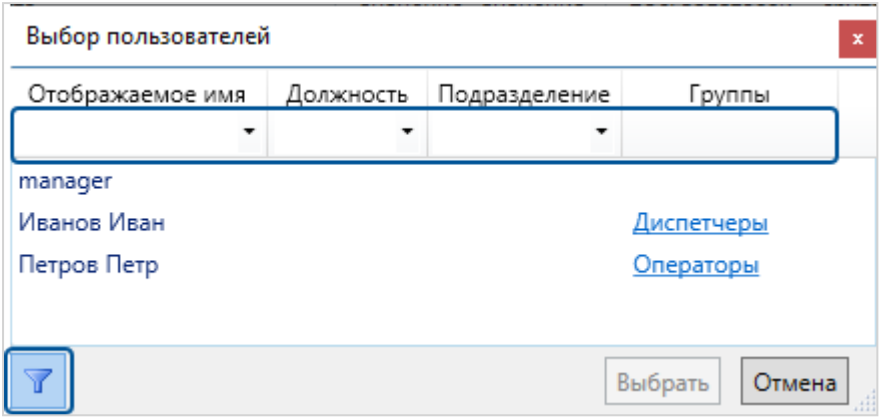
Фильтровать список пользователей

Фильтрация списка пользователей облегчает поиск пользователей в списке. Фильтровать список можно в разделе **Пользователи**, а также при добавлении пользователей в группы. Отображение нужных столбцов настраивается в контекстном меню.

› Чтобы отфильтровать пользователей в разделе **Пользователи**, нажмите **Фильтр** на панели инструментов. Появится строка для ввода названия искомого элемента.

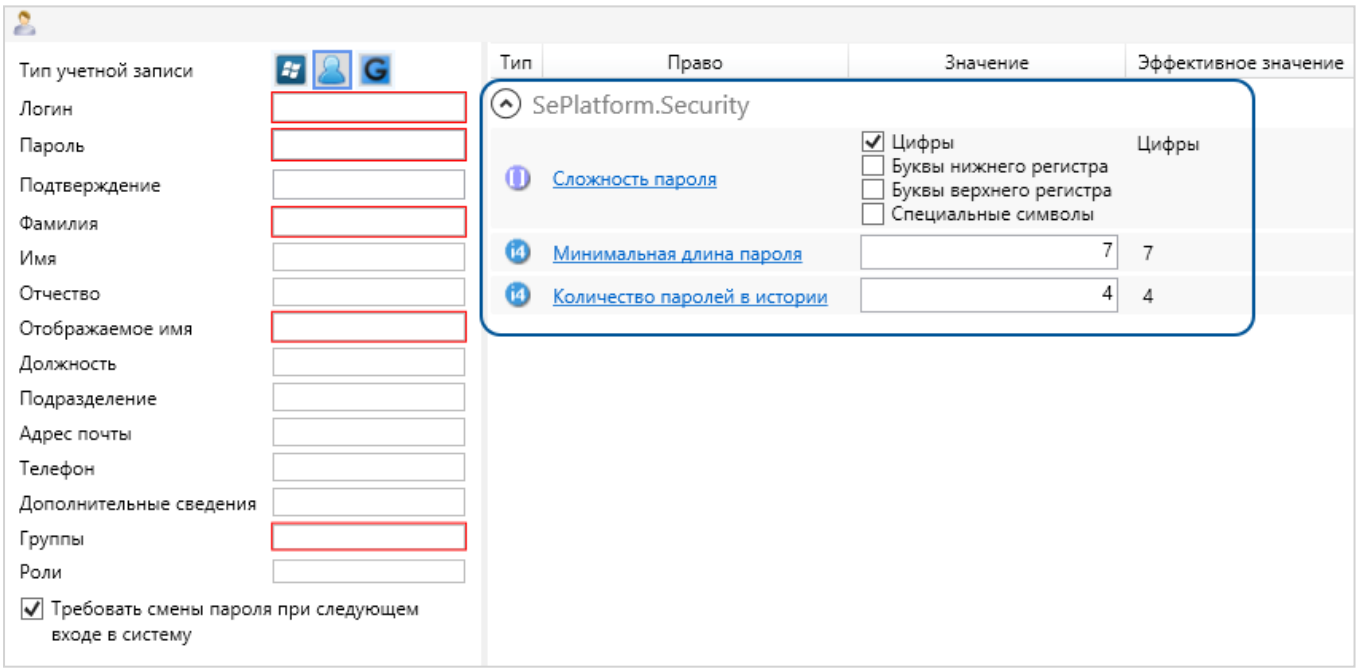


› Чтобы фильтровать пользователей при добавлении их в группу или назначая право, в окне **Выбор пользователей** нажмите иконку **Фильтр**. Появится строка для ввода названия искомого элемента.



Изменить начальные значения прав на уровне приложения

При создании новой учетной записи пользователя некоторые права добавляются автоматически. Это права, управляющие сложностью пароля, его длиной и количеством паролей, хранимых в истории учетной записи.



Настройка начальных значений этих прав возможна в конфигурационном файле `defaultPassReq.xml`, расположенном в `C:\ProgramData\SePlatform\SePlatform.SecurityConfigurator`. Меняя содержание файла, можно самостоятельно решать, будут ли добавляться эти права автоматически, и с какими начальными значениями.

ОБРАТИТЕ ВНИМАНИЕ

Перед редактированием конфигурационного файла нужно закрыть SecurityConfigurator.

После редактирования файла:

- при создании новых пользователей для автоматически назначенных прав будут установлены новые значения;
- у существующих пользователей значения останутся прежними, пока изменения не будут сохранены в окне редактирования пользователя.

Ознакомьтесь с содержанием файла:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration ProductName="SePlatform.SecurityConfigurator" ProductVersion="">
 <Configurable Id="defaultPassReq">
  <DefaultPasswordRequirementsSettings>
   <DigitsRequired>true</DigitsRequired>
   <UpperRequired>false</UpperRequired>
   <LowerRequired>false</LowerRequired>
   <SpecialRequired>false</SpecialRequired>
   <MinimalPasswordLength>7</MinimalPasswordLength>
   <MinimalPasswordHistoryLength>4</MinimalPasswordHistoryLength>
   <IdentityConfirmation>true</IdentityConfirmation>
  </DefaultPasswordRequirementsSettings>
 </Configurable>
</Configuration>
```

Внутри элемента `<DefaultPasswordRequirementsSettings>` во вложенных элементах хранятся начальные значения прав, автоматически добавляемых новому пользователю при создании новой учетной записи. В таблице ниже описаны эти элементы и то, как они управляют соответствующими правами.

Элемент	На что влияет	Возможные значения	Примечание
<DigitsRequired> соответствует части права **Сложность пароля**	Требование к наличию цифр в пароле	› **«true»** - в пароле должна содержаться хотя бы одна цифра; › **«false»** - в пароле не обязательно использовать цифры.	Если **«false»** установить для всех элементов, составляющих право **Сложность пароля**, то это право не будет автоматически добавляться пользователю при создании учетной записи. Если **«true»** установлено хотя бы для одного элемента, всё право автоматически добавляется пользователю целиком.
<UpperRequired> соответствует части права **Сложность пароля**	Требование к наличию букв в верхнем регистре в пароле	› **«true»** - в пароле должна содержаться хотя бы одна буква в верхнем регистре; › **«false»** - в пароле не обязательно использовать буквы в верхнем регистре.	
<LowerRequired> соответствует части права **Сложность пароля**	Требование к наличию букв в нижнем регистре в пароле	› **«true»** - в пароле должна содержаться хотя бы одна буква в нижнем регистре; › **«false»** - в пароле не обязательно использовать буквы в нижнем регистре.	

Элемент	На что влияет	Возможные значения	Примечание
<SpecialRequired> соответствует части права **Сложность пароля**	Требование к наличию специальных символов в пароле Перечень специальных символов приведен в Приложение D: Права стандартного приложения SePlatform.Security (стр. 109) (см. описание права **SpecialCount**)	› **«true»** - в пароле должен содержаться хотя бы один специальный символ; › **«false»** - в пароле не обязательно использовать специальные символы.	
<MinimalPasswordLength> соответствует праву **Минимальная длина пароля**	Требование к количеству символов в пароле	Любое значение типа int4.	Чтобы право не добавлялось автоматически при создании новой учетной записи, необходимо указать значение **«0»**. › Если уменьшить значение, указанное в файле, то у уже существующих пользователей будет указано старое значение права, но с возможностью уменьшить или удалить это значение. › Если увеличить значение, указанное в файле, то у уже существующих пользователей в качестве значения права будет указано новое значение из файла.
<MinimalPasswordHistoryLength> соответствует праву **Количество паролей в истории**	Требование к количеству паролей, хранимых в истории	Любое значение типа int4.	

Элемент	На что влияет	Возможные значения	Примечание
`<IdentityConfirmation>` Параметр, регулирующий необходимость подтверждения личности при запуске конфигуратора при наличии активной пользовательской сессии	-	-	Описано в Подключение к LDAP-серверу с помощью агента безопасности (стр. 50)

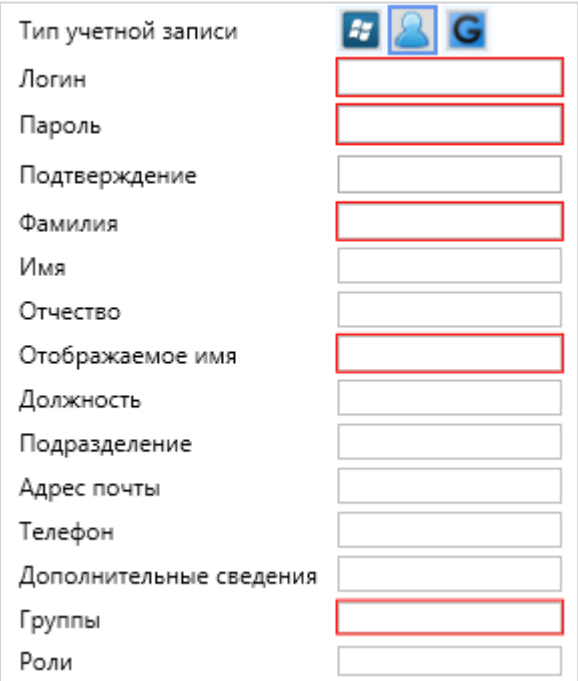
ПРИМЕР

Если не менять файл, то при создании новой учетной записи права назначаются автоматически.

Выставим значения **«false»** и **«0»** у всех элементов для того, чтобы отключить автоматическое назначение прав:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration ProductName="SePlatform.SecurityConfigurator"
ProductVersion="">
 <Configurable Id="defaultPassReq">
  <DefaultPasswordRequirementsSettings>
   <DigitsRequired>false</DigitsRequired>
   <UpperRequired>false</UpperRequired>
   <LowerRequired>false</LowerRequired>
   <SpecialRequired>false</SpecialRequired>
   <MinimalPasswordLength>0</MinimalPasswordLength>
   <MinimalPasswordHistoryLength>0</MinimalPasswordHistoryLength>
   <IdentityConfirmation>true</IdentityConfirmation>
  </DefaultPasswordRequirementsSettings>
 </Configurable>
</Configuration>
```

Тогда при создании новой учетной записи ни одно право не будет добавлено автоматически:



6.6. Назначение и указание значений прав

Право может быть назначено:

- пользователю лично - в окне редактирования учетной записи пользователя или в окне редактирования прав;
- группе пользователей - в окне редактирования группы или в окне редактирования прав;
- роли - в разделе приложений.

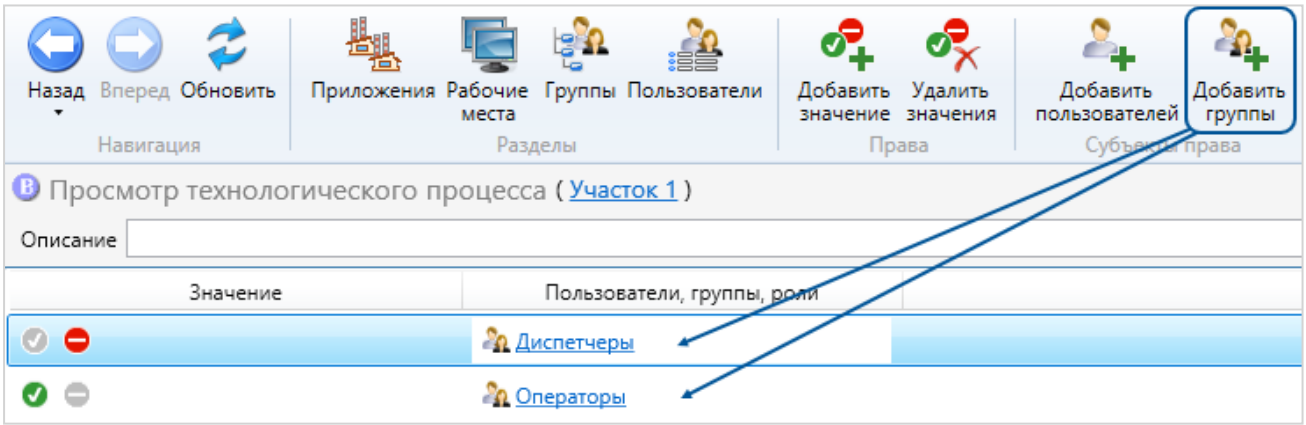
При назначении права указывается значение права. Итоговое значение права для пользователя зависит от того, какое значение права указано ему лично, в каких группах он состоит и какие роли ему назначены. Такое значение называется эффективным значением права. Подробнее об этом в Получить эффективное значение права (стр. 74).

Назначить право группе

Назначить право группе можно или в окне редактирования права, или в окне редактирования группы.

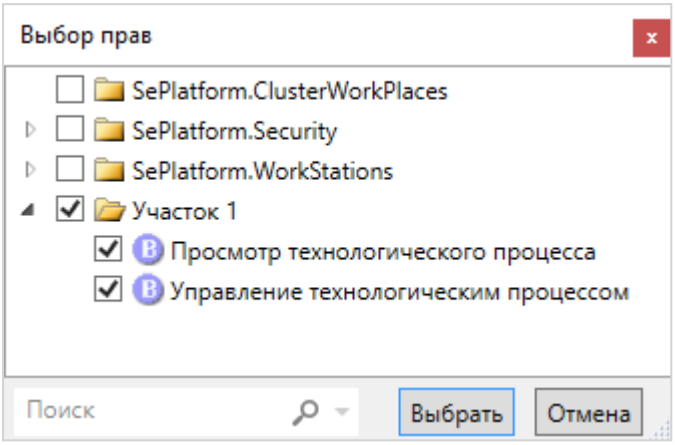
В окне редактирования права:

1. Нажмите **Добавить значение**. Появится строка с неопределенным значением права.
2. Выберите строку и нажмите **Добавить группы**. В диалоговом окне выберите нужные группы.
3. Укажите значение права для добавленной группы:
   - **«разрешено»** или **«запрещено»** - для логического права;
   - разрешающее значение и запрещающее значение - для строкового права.



В окне редактирования группы:

1. Нажмите **Добавить права**.
2. В диалоговом окне разверните приложение, права из которого необходимо назначить группе, и выберите нужные права.



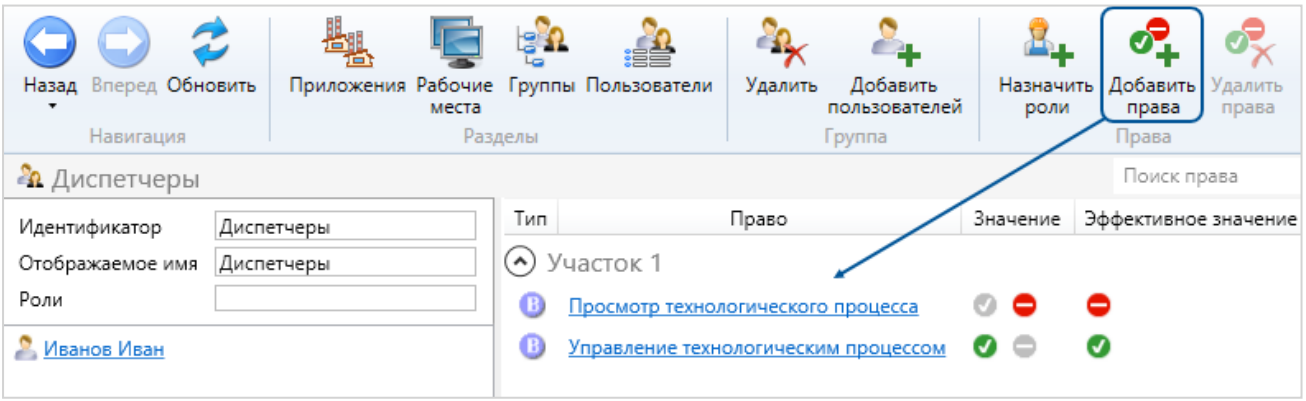
В редакторе группы появятся строки прав с неопределенными значениями.

ОБРАТИТЕ ВНИМАНИЕ

Приложение **SePlatform.Security** - это системное приложение, оно содержит системные права. Их можно назначить группе, например, чтобы разрешить просмотр и редактирование конфигурации всем пользователям в группе. Подробнее каждое право описано в Приложение D: Права стандартного приложения SePlatform.Security (стр. 109).

Приложения **SePlatform.ClusterWorkPlaces** и **SePlatform.WorkStations** содержат права доступа к кластерным рабочим местам и АРМ. Подробнее об их использовании читайте в 6.7. Организация кластерного рабочего места (стр. 75).

3. Укажите значения добавленных прав для группы:
   - **«разрешено»** или **«запрещено»** - для логического права;
   - разрешающее значение и запрещающее значение - для строкового права.



ПРИМЕР

Для пробной конфигурации назначьте права группам и укажите значения следующим образом:

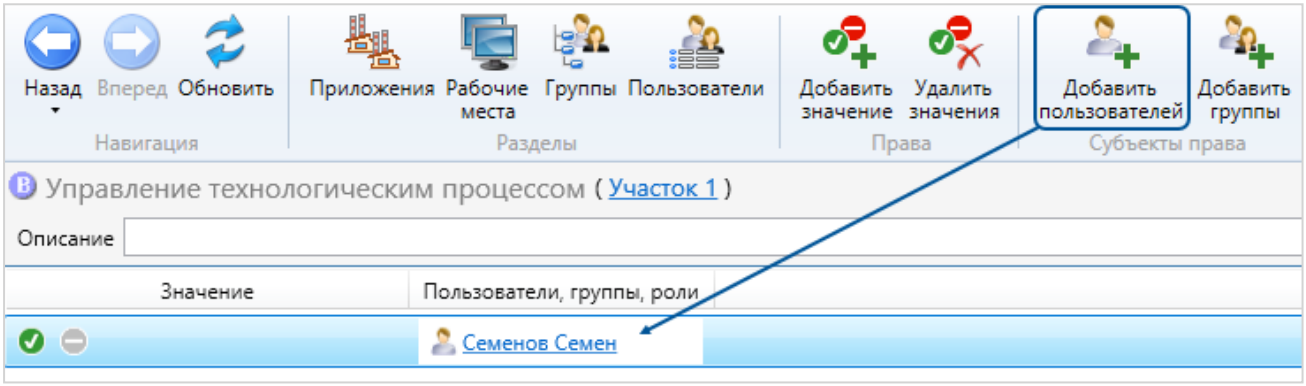
- группе **«Операторы»** разрешен **«Просмотр технологического процесса»** и запрещено **«Управление технологическим процессом»**;
- группе **«Диспетчеры»** запрещен **«Просмотр технологического процесса»** и разрешено **«Управление технологическим процессом»**;
- значения прав для группы **«Начальники участка»** оставьте неопределенными.

Назначить право пользователю

Назначить право пользователю можно или в окне редактирования права, или в окне редактирования учетной записи пользователя.

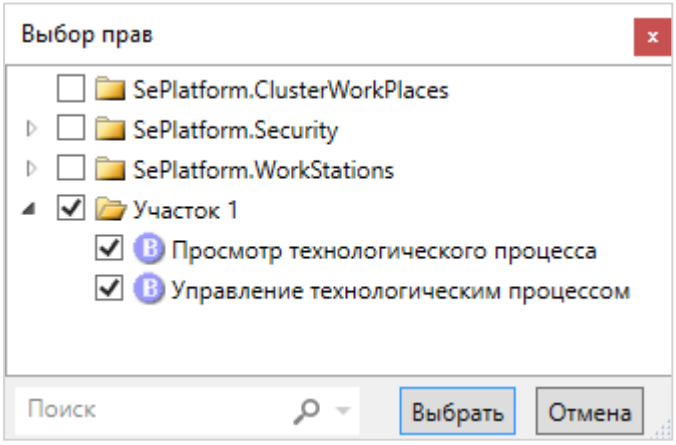
В окне редактирования права:

1. Нажмите **Добавить значение**. Появится строка с неопределенным значением права.
2. Выберите строку и нажмите **Добавить пользователей**. В диалоговом окне выберите нужных пользователей.
3. Укажите значение права для добавленных пользователей:
   - **«разрешено»** или **«запрещено»** - для логического права;
   - разрешающее значение и запрещающее значение - для строкового права.



В окне редактирования учетной записи:

1. Нажмите **Добавить права**.
2. В диалоговом окне разверните приложение, права из которого необходимо назначить группе, и выберите нужные права.



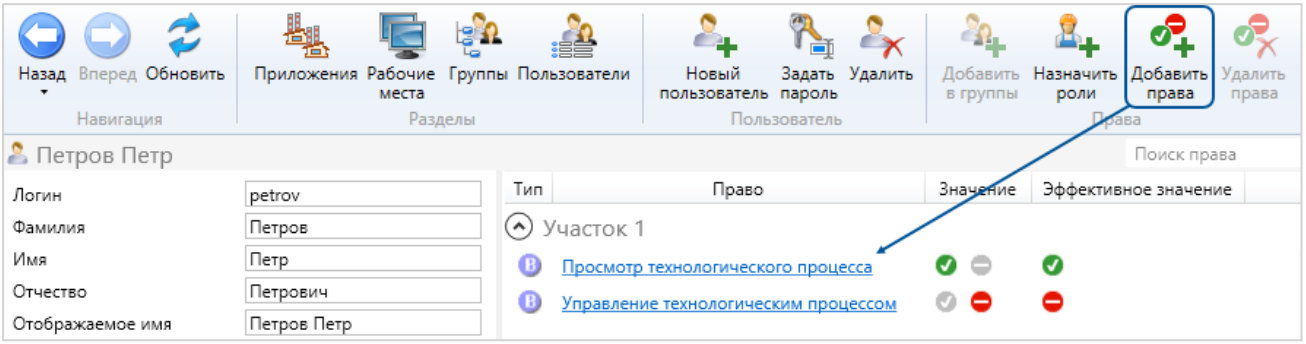
В редакторе учетной записи появятся строки прав с неопределенными значениями.

ОБРАТИТЕ ВНИМАНИЕ

Приложение **SePlatform.Security** - это системное приложение, оно содержит системные права. Их можно назначить пользователю, например, чтобы разрешить просмотр и редактирование конфигурации, или ограничить длительность сессии пользователя. Подробнее каждое право описано в Приложение D: Права стандартного приложения SePlatform.Security (стр. 109).

О приложениях **SePlatform.ClusterWorkPlaces** и **SePlatform.WorkStations** и их использовании читайте в 6.7. Организация кластерного рабочего места (стр. 75).

3. Укажите значения добавленных прав для группы:
   - **«разрешено»** или **«запрещено»** - для логического права;
   - разрешающее значение и запрещающее значение - для строкового права.



Получить эффективное значение права

Значение одного и того же права может быть назначено:

- пользователю лично;
- группе пользователей;
- роли.

В зависимости от того, в какой группе состоит пользователь и какая роль ему назначена, зависит эффективное значение права.

Правила определения эффективного значения права:

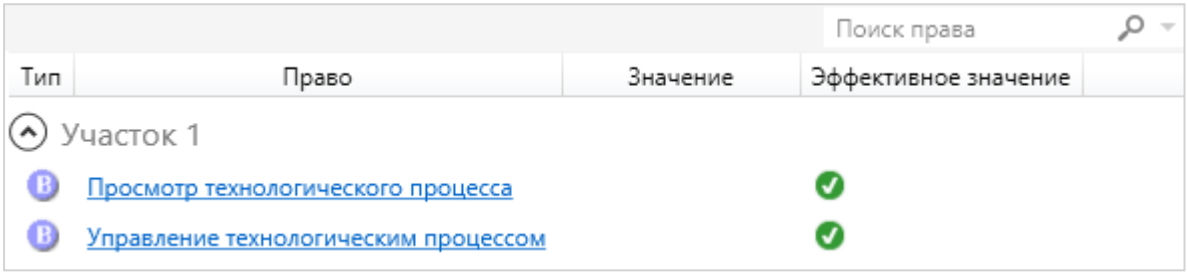
- Для булевского права:
  - если есть хоть одно разрешающее значение и нет запрещающих, эффективное значение разрешающее;
  - если есть хоть одно запрещающее значение, эффективное значение запрещающее.
- Для строковых прав эффективное значение складывается из всех наследованных прав. Строковые права отображаются списком.
- Эффективные значения для системных прав **`SePlatform.Security`** в Приложение D: Права стандартного приложения SePlatform.Security (стр. 109).

ПРИМЕР

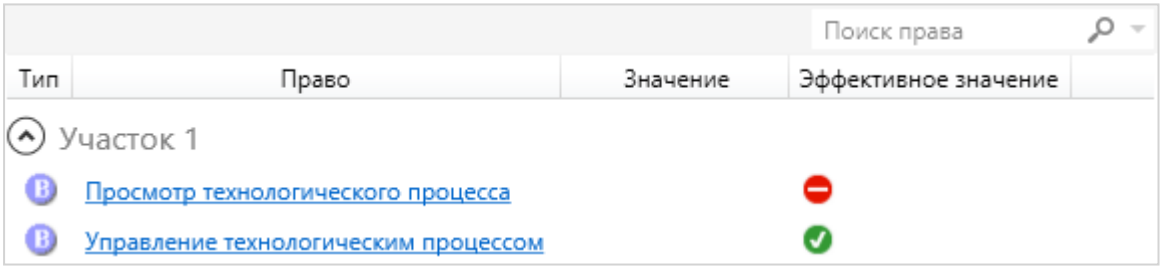
Перейдите к редактированию учетной записи пользователя **«Семенов Семен»**, состоящего в группе **«Начальники участка»** и обладающего ролью **«Начальник участка»**. Обратите внимание, что:

- ни одно право не было назначено пользователю лично;
- пользователь состоит в группе **«Начальники участка»**, которой назначены оба права приложения **«Участок 1»**, но не указаны значения прав;
- пользователю назначена роль **«Начальник участка»**, обладающая разрешениями обоих прав приложения **«Участок 1»**.

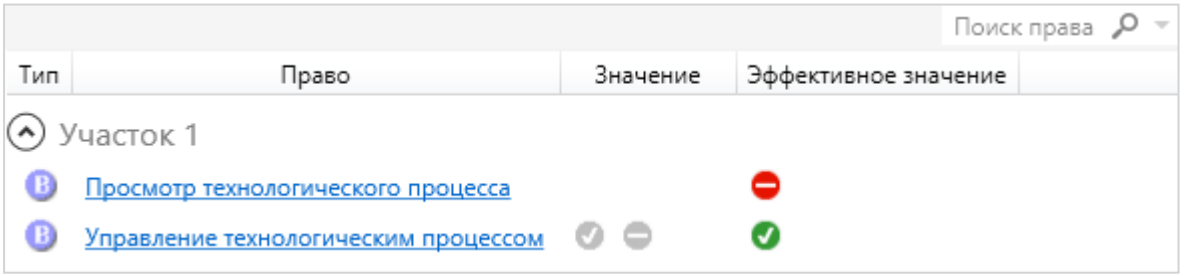
В столбце **Эффективное значение** обоих прав - **«разрешено»**, столбец **Значение** пустует.



Укажите группе **«Начальники участка»** запрещающее значение права **«Просмотр технологического процесса»**. Затем вернитесь к редактированию учетной записи начальника участка. Согласно правилу определения эффективного значения права, пользователю будет запрещено наблюдать за технологическим процессом.



Добавьте пользователю лично право **«Управление технологическим процессом»**. В строке права заполнится столбец **Значение**. Здесь можно указать значение права лично для пользователя.



6.7. Организация кластерного рабочего места

Несколько АРМ можно объединить в кластерное рабочее место. Тогда после входа с учетными данными на одном АРМ, вход автоматически произойдет на остальных АРМ, входящих в кластерное рабочее место.

Чтобы создать кластерное рабочее место, необходимо:

1. Объединить АРМ, входящие в кластерное рабочее место, в сеть SePlatform.Net.
2. Настроить Агент SePlatform.Security всех АРМ на общий LDAP-сервер.
3. Создать кластерное рабочее место, используя SecurityConfigurator.

Когда кластерные рабочие места будут созданы, доступ к кластерным местам и АРМ можно будет назначать пользователям и группам в виде прав приложений **SePlatform.ClusterWorkPlaces** и **SePlatform.WorkStations**.

Объединить АРМ в сеть SePlatform.Net

Перед началом настройки определите АРМ, который будет центральным узлом сети SePlatform.Net: на центральном узле сети создана нужная конфигурация LDAP-сервера (пользователи, группы, приложения и права). Настройки центрального узла будут отличаться от настроек остальных АРМ.

ОБРАТИТЕ ВНИМАНИЕ

Ниже описано создание простейшей сети SePlatform.Net, в которой все узлы соединяются с центральным узлом сети. Более сложные схемы сети SePlatform.Net следует использовать только если центральный узел сети не имеет сетевого соединения с каким-либо другим узлом (например, если компьютеры находятся в разных сетях, между которыми работает брандмауэр). В данном примере такие схемы не рассматриваются.

На каждом АРМ:

1. Установите SePlatform.Net (входит в дистрибутив SePlatform.Domain).
2. Сконфигурируйте SePlatform.Net:

   2.1. Перейдите в папку установки `C:\Program Files\SePlatform\SePlatform.Domain` и откройте файл конфигурации `seplatform.net.agent.xml` в любом текстовом редакторе.

   2.2. В атрибутах элемента **SePlatform.Net.Agent** укажите параметры АРМ в сети SePlatform.Net.

Атрибут	Описание
Name	Имя АРМ в сети SePlatform.Net. Должно быть уникальным в сети SePlatform.Net.
NetEnterPort	Порт, по которому другие службы соединяются с данным узлом (по умолчанию - **«1010»**).
ParentAgentPort	Порт для соединения с центральным узлом сети SePlatform.Net. Рекомендуется разным узлам назначать разные значения атрибута. У центрального узла сети указывать не обязательно.

ПРИМЕР

Центральный узел:

```
<SePlatform.Net.Agent Name="CentralNode" NetEnterPort="1010" >
```

Остальные АРМ в сети:

```
<SePlatform.Net.Agent Name="ARM1" NetEnterPort="1010"
ParentAgentPort="1009">
```

```
<SePlatform.Net.Agent Name="ARM2" NetEnterPort="1010"
ParentAgentPort="1090">
```

2.3. На центральном узле сети SePlatform.Net, в этом же файле, раскомментируйте конструкцию `<ChildAgents>` и перечислите все дочерние узлы сети, указав их параметры:

Атрибут	Описание
Name	Имя дочернего узла сети SePlatform.Net. Указано в конфигурации дочернего узла в атрибуте **Name**.
Address	IP-адрес дочернего узла сети SePlatform.Net.
Port	Номер порта для подключения к дочернему узлу. Указан в конфигурации дочернего узла в атрибуте **ParentAgentPort**.

ПРИМЕР

```
<SePlatform.Net.Agent Name="CentralNode" NetEnterPort="1010" >
 <ChildAgents>
  <ChildAgent Name="ARM1" Address="199.99.99.101" Port="1009"/>
  <ChildAgent Name="ARM2" Address="199.99.99.102" Port="1090"/>
 </ChildAgents>
 <Options LoggerLevel="2"/>
</SePlatform.Net.Agent>
```

2.4. Перезапустите службу **SePlatform.Net.Agent**, чтобы применить внесённые изменения.

В результате АРМ будут объединены в сеть SePlatform.Net.

Настроить Агент SePlatform.Security на общий LDAP-сервер

На всех АРМ сети должен быть установлен SePlatform.Security. При этом каждый Агент SePlatform.Security должен быть настроен на один и тот же каталог LDAP-сервера центрального узла.

На каждом дочернем узле сети:

1. Установите SePlatform.Security;
2. Перейдите к настройке Агент SePlatform.Security. Откройте конфигурационный файл `seplatform.security.agent.xml`, расположенный в `C:\Program Files\SePlatform\SePlatform.Security` и укажите:
   2.1. Параметры локальной точки доступа Net-агента, входящей в сеть SePlatform.Net:

ПРИМЕР

```
<EntryPointNetAgent Address="127.0.0.1" Port="1010"/>
```

   2.2. Параметры LDAP-сервера, развернутого на центральном узле сети:

ПРИМЕР

```
<LdapHosts>
 <LDAPServer Address="199.99.99.111" Port="389"/>
</LdapHosts>
```

   2.3. Администратора LDAP, пароль администратора и корневой каталог - такие же, как в настройках Агент SePlatform.Security на центральном узле сети.

ПРИМЕР

```
<!-- Каталог пользователя LDAP -->
<LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>
<!-- Пароль LDAP -->
<LdapPassword value="..."/>
<!-- Корневой каталог -->
<SecurityDn value="ou=Security,dc=maxcrc,dc=com"/>
```

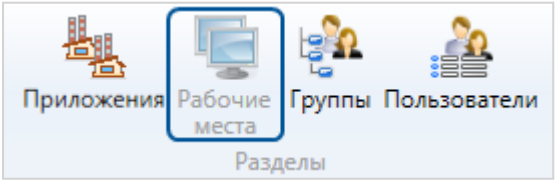
3. Перезапустите службу **`SePlatform.Security.Agent`**, чтобы применить внесённые изменения.

В результате АРМ сети будут настроены на общий LDAP-сервер.

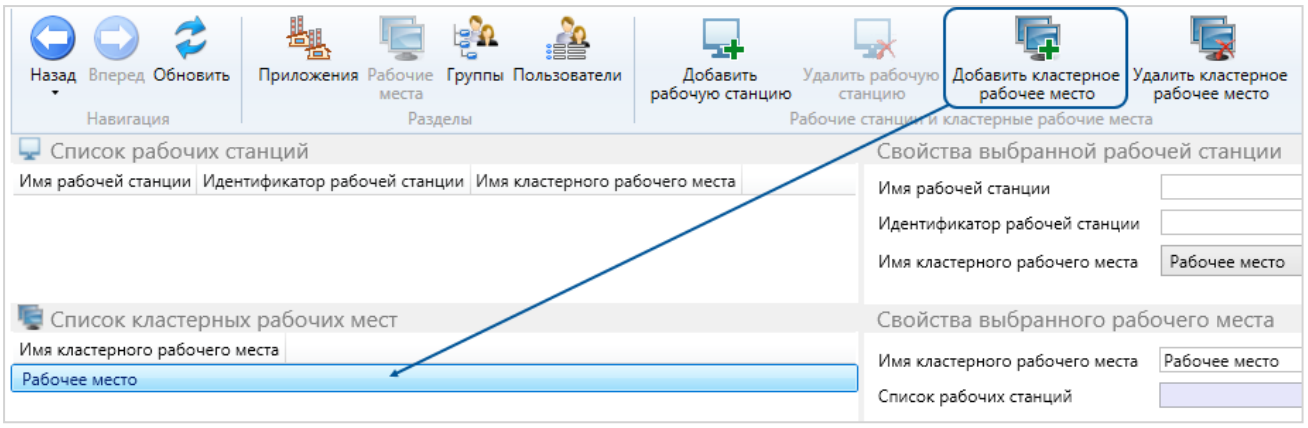
Создать кластерное рабочее место

Кластерное рабочее место создаётся в SecurityConfigurator:

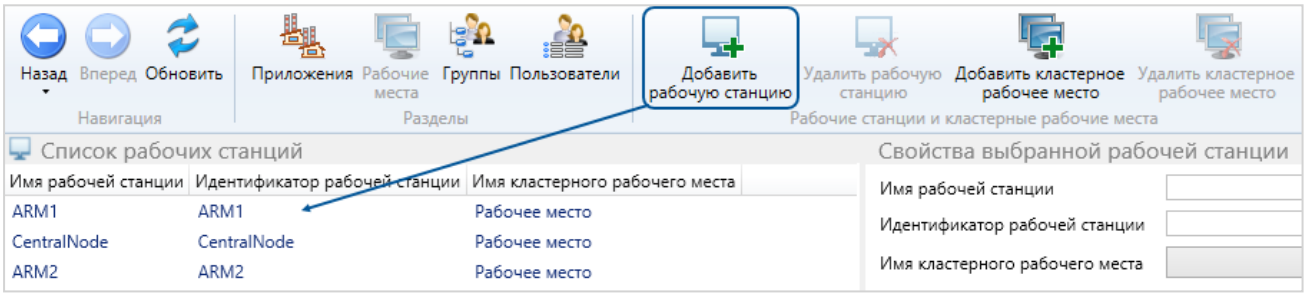
1. На панели инструментов выберите **`Рабочие места`**.



2. Добавьте кластерное рабочее место.

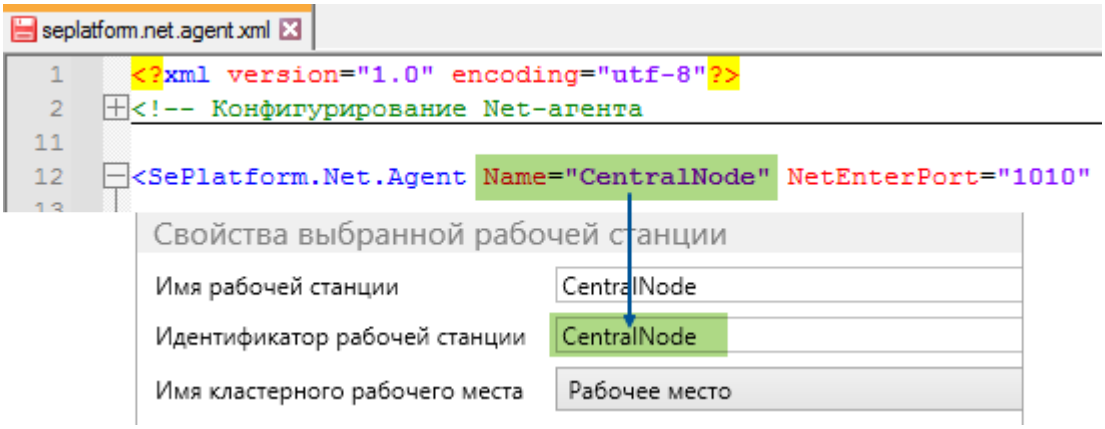


3. Для каждого АРМ, который войдёт в кластерное рабочее место, добавьте рабочую станцию и укажите свойства.



Свойства

Параметр	Описание
Имя рабочей станции	Произвольное имя.
Идентификатор рабочей станции	Имя АРМа в сети SePlatform.Net. Совпадает со значением атрибута **Name** в файле конфигурации SePlatform.Net.
Имя кластерного рабочего места	Выберите кластерное рабочее место, добавленное ранее.



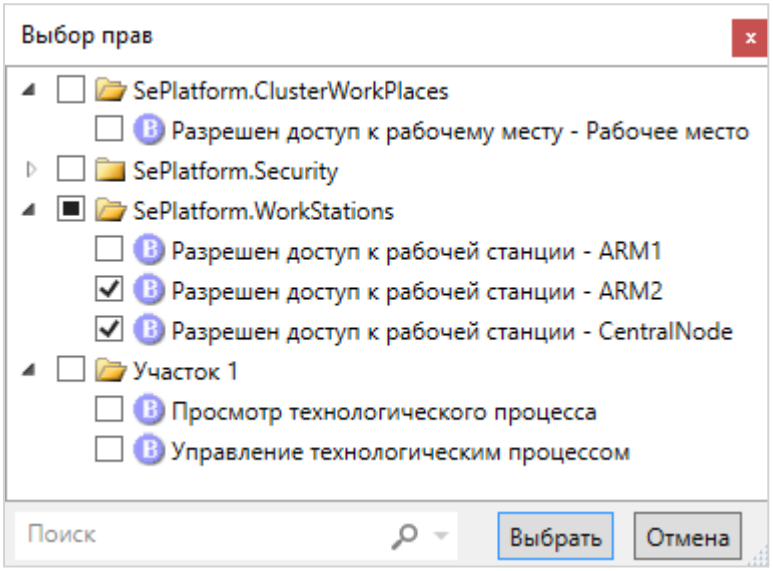
В результате будет создано кластерное рабочее место, в которое входят АРМ из числа объединенных в сеть SePlatform.Net.

Предоставить доступ к кластерным рабочим местам и АРМ пользователям

Права доступа к созданным кластерным рабочим местам и АРМ хранятся в приложениях **`SePlatform.ClusterWorkPlaces`** и **`SePlatform.WorkStations`** соответственно. Права создаются автоматически в момент создания соответствующих элементов.

Назначить права доступа можно как пользователям, так и группам:

- **`Разрешен доступ к рабочему месту`** - право доступа к кластерному рабочему месту.
- **`Разрешен доступ к рабочей станции`** - право доступа к отдельному АРМ.

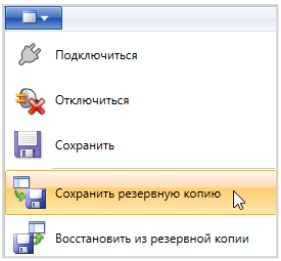
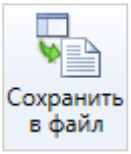


В результате возможность авторизоваться на всех АРМ, входящих в кластерное рабочее место, зависит от комбинации назначенных прав.

Доступ к кластерному рабочему месту	**Доступ к АРМ, входящим в кластерное рабочее место**	**Результат авторизации**
Есть	Есть, ко всем	При входе на одном из АРМ авторизация происходит на всех АРМ, входящих в кластерное рабочее место.
	Есть, не ко всем	При входе на одном из АРМ, к которому есть доступ, авторизация происходит только на тех АРМ, к которым имеется доступ.
Нет	Есть	При входе на одном из АРМ не происходит авторизация на остальных АРМ.

6.8. Резервное копирование конфигурации

Информацию из каталогов LDAP можно сохранять в резервные копии. Они могут пригодиться при переносе конфигурации на другие АРМ, для создания отчетов и пр. Используйте SecurityConfigurator для создания резервных копий. Способы создания и варианты использования копий описаны в таблице ниже.

Что сохранить	Формат файла	Как сохранить	Как использовать
Полная резервная копия конфигурации	`*.bak`	**Меню -> Сохранить резервную копию** 	Можно восстановить конфигурацию из резервной копии: **Меню -> Восстановить из резервной копии**
Список приложений и прав	`*.xml`	Раздел **Приложения -> Сохранить в файл** 	Можно импортировать приложения и права из сохраненного файла: **Приложения -> Добавить из файла**

	`*.xlsx`
	`*.csv`
	`*.docs`
		Раздел **Приложения -> Экспорт в Excel**
		 
			В качестве отчета о разрешениях и запретах пользователей и групп пользователей

Список пользователей	`*.xlsx`
	`*.xml`
	`*.csv`
	`*.docs`
		Раздел **Приложения -> Экспорт в Excel**
		 
			Во всех случаях, когда нужен список пользователей со всеми данными пользователей

7. Аудит безопасности

SePlatform.Security может отправлять сообщения об изменениях в подсистеме безопасности в сигналы SePlatform.Data Server. Эта функция называется аудитом безопасности.

Для получения сообщений аудита безопасности необходимы:

- SePlatform.Security – транслирует сообщения;
- SePlatform.Data Server с подключенным модулем OPC AE Server – записывает сообщения в сигналы;
- любое средство просмотра значений сигналов сервера (Service - OPCExplorer) или сообщений (Service - LogViewer, SePlatform.HMI.Alarms).

Сообщения аудита безопасности бывают трех типов:

- первые сообщают об изменениях в списках пользователей, групп и приложений, в т.ч. прав и ролей;
- вторые – служебные сообщения о работе Агент SePlatform.Security (вход и выход пользователя, выполнение контроля целостности и пр.);
- третьи хранят информацию о текущем пользователе (логин, отображаемое имя, группа) и рабочей станции.

Чтобы ознакомиться с сообщениями первых двух типов, перейдите к файлу `seplatform.security.agent.json`, расположенному в:

- `C:\Program Files\SePlatform\SePlatform.Security` – для ОС Windows;
- `/opt/SePlatform/SePlatform.Security` – для ОС Linux.

Сообщениями третьего типа являются:

- логин текущего пользователя;
- отображаемое имя текущего пользователя;
- название группы, в которой состоит текущий пользователь;
- имя текущей рабочей станции.

Чтобы получать сообщения о состоянии подсистемы безопасности, необходимо:

- настроить Агент SePlatform.Security для трансляции сообщений, при необходимости изменив тексты сообщений;
- подготовить сигналы в SePlatform.Data Server.

Настройка Агент SePlatform.Security и редактирование текстов сообщений

Для настройки аудита безопасности и его сообщений следует редактировать конфигурационные файлы `seplatform.security.agent.json` и `seplatform.security.agent.xml`, расположенные в:

- `C:\Program Files\SePlatform\SePlatform.Security` – для ОС Windows;
- `/opt/SePlatform/SePlatform.Security` – для ОС Linux.

Редактирование текстов сообщений

Файл `seplatform.security.agent.json` хранит тексты сообщений, которые можно редактировать. При формировании текста сообщения можно использовать теги. Теги описаны в начале файла. Для каждого сообщения указаны параметры, назначение которых описано в таблице ниже.

Название параметра	Назначение параметра
`name`	Идентификатор сообщения. Менять нельзя.
`value`	Текст сообщения.
`type`	Тип сообщения. Тип служит для пометки сообщений, которые могут быть записаны в один и тот же сигнал SePlatform.Data Server. По умолчанию все сообщения имеют тип `Admin` и записываются в один и тот же сигнал, указанный в карте сигналов конфигурационного файла `seplatform.security.agent.xml`. Чтобы разные сообщения записывались в разные сигналы, одним сообщениям необходимо указать тип `Admin`, а другим - `Normal`, а затем в карте сигналов указать эти типы для разных сигналов. Названия `Admin` и `Normal` можно менять, главное - чтобы новые названия были указаны в обоих конфигурационных файлах.
`severity`	Категория важности сообщения. Этот параметр служит для разделения всех сообщений на четыре категории важности. Категории описаны в карте важности конфигурационного файла `seplatform.security.agent.xml`. По умолчанию для всех сообщений указана категория важности `Info`.
`sound`	Звук, который должен быть воспроизведен при наступлении события, о котором говорится в сообщении. Формат значения - имя и расширение файла звука. Файл звука должен находиться в папке проекта, посредством которого просматриваются события, например, SePlatform.HMI.Alarms. Подробнее об этом - в документе на соответствующий продукт.
`ackrequired`	Необходимость квитирования события, о котором говорится в сообщении. Если необходимо квитировать событие, укажите значение **«1»**, если нет - **«0»**.

ПРИМЕР

По умолчанию сообщение описано следующим образом:

```
{"name":"AUDIT_ADD_USER", "value":"На '%arm.name%' от имени
'%currUser.symbolicId%' группа '%currGroup.symbolicId%': Настройка списка
пользователей - Добавлен пользователь '#user.displayName#'.", "type":"Admin",
"severity":"Info", "sound":"", "ackrequired":"0"}
```

Здесь можно изменить текст сообщения, тип и важность, указать звук и необходимость квитирования:

```
{"name":"AUDIT_ADD_USER", "value":"В группу '%currGroup.symbolicId%' добавлен
пользователь '#user.displayName#'.", "type":"Normal", "severity":"Debug",
"sound":"defaul.wav", "ackrequired":"1"}
```

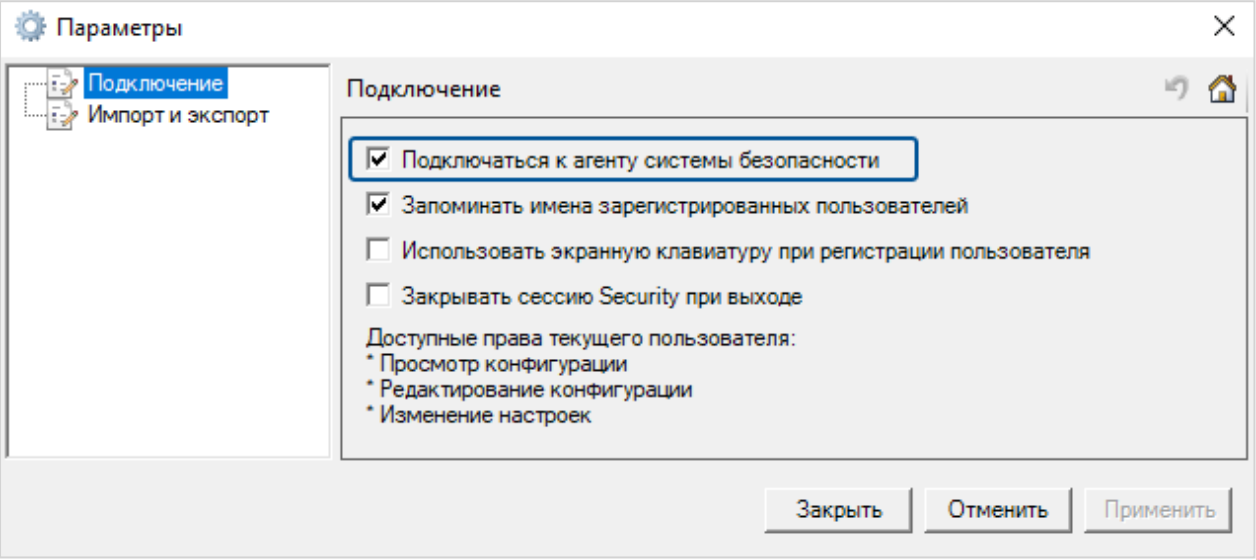
ПРИМЕЧАНИЕ

Сообщения первого типа отправляются в результате изменений, произведенных в конфигураторе безопасности.

SePlatform.HMI.SecurityConfigurator транслирует сообщения аудита первого типа, перечисленные в `seplatform.security.agent.json`.

SecurityConfigurator транслирует собственные сообщения аудита первого типа, поэтому изменить их не получится.

Чтобы пользоваться функцией аудита безопасности, включите в настройках SecurityConfigurator подключение к агенту безопасности.



Настройка агента безопасности для трансляции сообщений

Файл `seplatform.security.agent.xml` позволяет настроить и включить трансляцию сообщений. Для этого:

1. Откройте файл. Перейдите к элементу `<AuditLogConsumers>`. Включите трансляцию сообщений, задав значение атрибута `TraceAudit`:
   - **«1»** - для включения аудита;
   - **«0»** - для отключения аудита.

```
<AuditLogConsumers TraceAudit="0">
```

2. Во вложенном элементе `<OpcDaLogConsumer>` опишите так называемый сервер-потребитель сообщений - экземпляр SePlatform.Data Server, в сигналы которого будут транслироваться сообщения. Укажите значения атрибутов элемента `<Server>`:

- `Host` - IP-адрес сервера;
- `Type` - тип сервера (**«OPC»** или **«TCP»** для Windows, только **«TCP»** для Linux);
- `ProgId` - строковый идентификатор OPC-сервера (если выбран OPC-сервер);
- `TCPServerPort` - порт для подключения к TCP-серверу (если выбран TCP-сервер);
- `HostTcpReserve` - имя или IP-адрес сервера для резервного канала связи с TCP-сервером (значение может быть пустым);
- `MasterPasswordCipher` - хэш-значение мастер-пароля, установленного на подключение к TCP-серверу (значение может быть пустым).

ПРИМЕЧАНИЕ

Это значение должно совпадать со значением атрибута `Cipher` элемента `<MasterPassword>` в файле настроек SePlatform.Data Server или SePlatform.AccessPoint:

```
<MasterPassword Cipher="bknxu/rPt/+PCnmzYA....lB1i2bHuzYk2/XKKYFr" />
```

```
<Server Host="127.0.0.1" Type="OPC" ProgId="SePlatform.OPCDAServer"
TCPServerPort="4388"
HostTcpReserve="" MasterPasswordCipher="">
```

ОБРАТИТЕ ВНИМАНИЕ

В рамках одного элемента `<OpcDaLogConsumer>` может быть настроен только один сервер-потребитель сообщений.

Количество элементов `<OpcDaLogConsumer>` может быть любым.

3. Задайте значения для каждой категории важности событий в карте важности `<SeverityMap>`, изменив значения атрибутов `Value`. Атрибут может принимать значения от 0 до 999. Обратите внимание, что эти значения понадобятся в дальнейшем - например, при настройке событий в сигналах SePlatform.Data Server, при настройке отображения событий в SePlatform.HMI.Alarms.

Таким образом можно отметить, какие сообщения имеют высокую важность, а какие - низкую. По умолчанию всем сообщениям в файле `seplatform.security.agent.json` указана категория важности **«Info»**.

```
<SeverityMap>
 <Severity Category="Critical" Value="800" Sound=""/>
 <Severity Category="Important" Value="200" Sound=""/>
 <Severity Category="Info" Value="100" Sound=""/>
 <Severity Category="Debug" Value="0" Sound=""/>
</SeverityMap>
```

Здесь же для каждой категории в качестве значения атрибута `Sound` можно указать файл звука, который должен быть воспроизведен при наступлении события из этой категории. Звук может быть указан либо для категории важности, либо для каждого сообщения о событии отдельно - в файле `seplatform.security.agent.json`, как описано выше. Если для сообщения не указан звук, то при наступлении события воспроизводится звук, указанный для категории важности этого события. Файл звука должен находиться в папке проекта, посредством которого просматриваются события, например, SePlatform.HMI.Alarms. Подробнее об этом - в документе на соответствующий продукт.

4. Заполните значения атрибутов карты сигналов `<SignalMap>`. В указанные здесь сигналы и записываются сообщения аудита. Обратите внимание, что названия сигналов могут быть любыми. Важно, чтобы для каждого типа - `Normal`, `Admin`, `UserName`, `DisplayName`, `GroupName` и `WorkstationName` - было создано по два сигнала с разным режимом записи. Подробнее назначения атрибутов карты описаны в таблице ниже.

```
<SignalMap>
 <Signal Name="DynEvents.NormalDynSignal" Mode="DynamicEvent" Type="Normal"/>
 <Signal Name="DynEvents.AdminDynSignal" Mode="DynamicEvent" Type="Admin"/>
 <Signal Name="DynEvents.UserNameDynSignal" Mode="DynamicEvent"
Type="UserName"/>
 <Signal Name="DynEvents.DisplayNameDynSignal" Mode="DynamicEvent"
Type="DisplayName"/>
 <Signal Name="DynEvents.GroupNameDynSignal" Mode="DynamicEvent"
Type="GroupName"/>
 <Signal Name="DynEvents.WorkstationNameDynSignal" Mode="DynamicEvent"
Type="WorkstationName"/>
 <Signal Name="DynEvents.NormalMessage" Mode="Value" Type="Normal"/>
 <Signal Name="DynEvents.AdminMessage" Mode="Value" Type="Admin"/>
 <Signal Name="DynEvents.UserNameMessage" Mode="Value" Type="UserName"/>
 <Signal Name="DynEvents.DisplayNameMessage" Mode="Value"
Type="DisplayName"/>
 <Signal Name="DynEvents.GroupNameMessage" Mode="Value" Type="GroupName"/>
 <Signal Name="DynEvents.WorkstationNameMessage" Mode="Value"
Type="WorkstationName"/>
</SignalMap>
```

Назначения атрибутов карты сигналов

Название атрибута	Назначение атрибута
`Name`	Полное имя сигнала как в SePlatform.Data Server.
`Mode`	Режим записи сообщения в сигнал: › **«`DynamicEvent`»** - сигнал, создающий динамическое событие; › **«`Value`»** - обычная запись сообщения.
`Type`	Тип сообщений, записывающихся в сигнал. Типы описаны в начале данного раздела. Для каждого сообщения третьего типа (`UserName`, `DisplayName`, `GroupName` и `WorkstationName`) создается по собственной паре сигналов. Для сообщений первого и второго типа достаточно двух пар сигналов. В этом случае атрибут `Type` служит для пометки сообщений, которые могут быть записаны в один и тот же сигнал. По умолчанию в файле `seplatform.security.agent.json` все сообщения имеют тип `Admin`, и записываются в один и тот же сигнал, указанный в карте сигналов. Чтобы разные сообщения записывались в разные сигналы, одним сообщениям необходимо указать тип `Admin`, а другим - `Normal`, а затем в карте сигналов указать эти типы для разных пар сигналов. Названия `Admin` и `Normal` можно менять, главное - чтобы новые названия были указаны в обоих конфигурационных файлах.

5. Дополнительно можно изменить префикс сообщений аудита, изменив значение атрибута `value` элемента `<mesPrefix>`. Он служит для выделения сообщений аудита безопасности в списке всех остальных сообщений, которые могут отображаться в средстве просмотра.

Подготовка сигналов в SePlatform.Data Server

Для каждого сообщения аудита необходимо создать по два сигнала: обычный и динамический. Динамический сигнал позволяет сгенерировать событие, отправляющее сообщение из обычного сигнала в средства просмотра сообщений.

Чтобы подготовить SePlatform.Data Server к записи сообщений подсистемы безопасности, необходимо создать 12 сигналов типа **`String`** в отдельной папке дерева сигналов. Имена сигналов по умолчанию перечислены в конфигурационном файле `seplatform.security.agent.xml`, но их можно изменить.

- Динамические сигналы, приведенные в конфигурационном файле по умолчанию:
  - Messages.NormalDynSignal;
  - Messages.AdminDynSignal;
  - Messages.UserNameDynSignal;
  - Messages.DisplayNameDynSignal;
  - Messages.GroupNameDynSignal;
  - Messages.WorkstationNameDynSignal.
- Обычные сигналы, приведенные в конфигурационном файле по умолчанию:
  - Messages.NormalMessage;
  - Messages.AdminMessage;
  - Messages.UserNameMessage;
  - Messages.DisplayNameMessage;
  - Messages.GroupNameMessage;
  - Messages.WorkstationNameMessage.

Создание сигналов в приложении Конфигуратор

Если для конфигурирования SePlatform.Data Server вы используете приложение **`Конфигуратор`**, то:

1. Создайте в дереве сигналов папку для сигналов аудита (например **`Messages`**). Внутри папки создайте 12 сигналов типа **`String`**.

2. Затем настройте генерацию событий при записи сообщений в сигналы. Для этого назначьте созданным объектам свойства, описанные в таблицах ниже. Также можно включить флаг ведения истории, чтобы иметь возможность обратиться к ней при перезаписи значения сигнала.

ПРИМЕЧАНИЕ

Для того, чтобы запись сообщения в сигнал генерировала событие, в конфигурацию SePlatform.Data Server должен быть включен модуль OPC AE Server. Подробнее о том, как подключить, настроить и использовать модуль, читайте в соответствующем документе.

› Папке **Messages**:

Свойство	Значение
999000 (тип объекта)	Можно не указывать.

999004 (условие генерации сообщений)	Скрипт, генерирующий сообщение при наступлении события.
	ПРИМЕР
	`<EventConditions>`
	`<EventCondition Name="DynamicCondition" Type="Dynamic" Enabled="1">`
	`<Subcondition Type="Dynamic" Message="" Value="" Sound="" Severity="100" AckRequired="0" Enabled="1" SoundEnabled="0" />`
	`</EventCondition>`
	`</EventConditions>`
	где:
	› значение атрибута `Name` будет использоваться при настройке динамических сигналов;
	› значение атрибута `Severity` должно совпадать со значением категории важности сообщений, записывающихся в сигнал, указанным при настройке агента.

› Динамическим сигналам (содержат частицу **«Dyn»** в названии по умолчанию):

Свойство	Значение
5000 (адрес сигнала)	`Conditions=(DynamicCondition)`, где название условия в скобках должно совпадать со значением атрибута `Name`, указанным в свойстве **999004** папки **Messages**.
9001 (флаг ведения истории)	`True`

› Обычным сигналам:

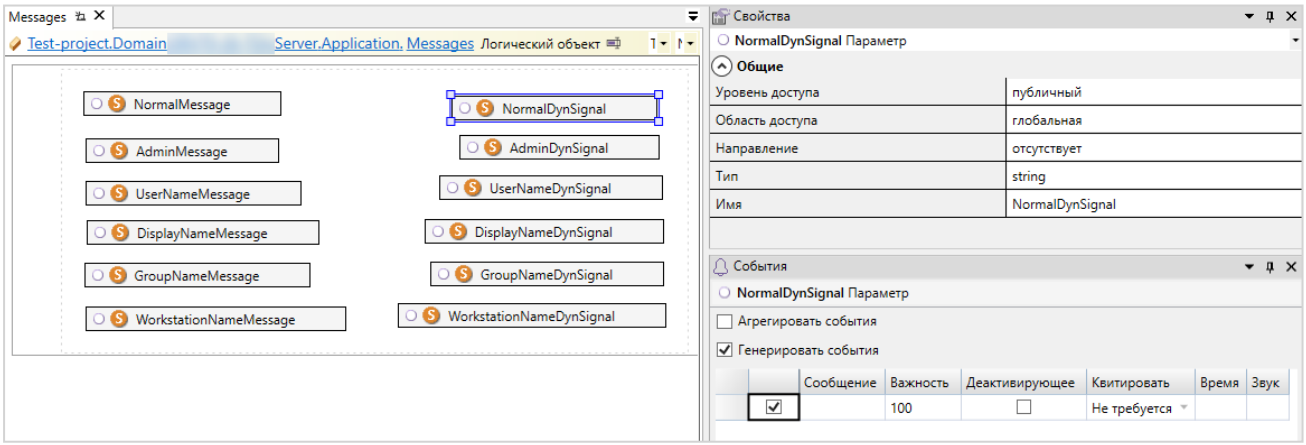
Свойство	Значение
9001 (флаг ведения истории)	`True`

Создание сигналов в SePlatform.Development Studio

> ПРИМЕЧАНИЕ
>
> Порядок создания проекта и конфигурирования SePlatform.Data Server описаны в документации на SePlatform.Development Studio (раздел **«Знакомство с SePlatform.Development Studio руководства пользователя»**). Здесь описано создание сигналов в уже сконфигурированном SePlatform.Data Server в существующем проекте.

Если для конфигурирования SePlatform.Data Server вы используете SePlatform.Development Studio, то:

1. Откройте имеющийся проект SePlatform.Development Studio. Перейдите к элементу, описывающему сервер в вашем проекте. Убедитесь, что здесь подключен элемент OPC AE Server.
2. Перейдите внутрь элемента, описывающего сервер. Здесь может быть размещен элемент приложения. Если его нет, создайте, перетянув элемент **Приложение** с панели элементов.
3. Внутри элемента приложения создайте логический объект. Это будет папка для сигналов, предназначенных для записи сообщений аудита (например **Messages**).
4. Внутри созданного логического объекта создайте двенадцать параметров, соответствующих двенадцати сигналам, предназначенным для записи сообщений аудита. Для всех параметров укажите значения свойств:
   - Направление (**«отсутсвует»**);
   - Тип (**«string»**);
   - Имя.
5. Для шести параметров, предназначенных для создания динамических событий, в окне **События** установите флаг **Генерировать события** (такие сигналы в именах по умолчанию содержат частицу **«Dyn»**). Чтобы открыть окно, перейдите к панели инструментов и выберите **Вид -> События**. В открывшейся таблице укажите значение важности события, соответствующее категории важности, указанной при конфигурировании агента. Если необходимо, укажите файл звука, воспроизводимого при наступлении события, и параметры квитирования.

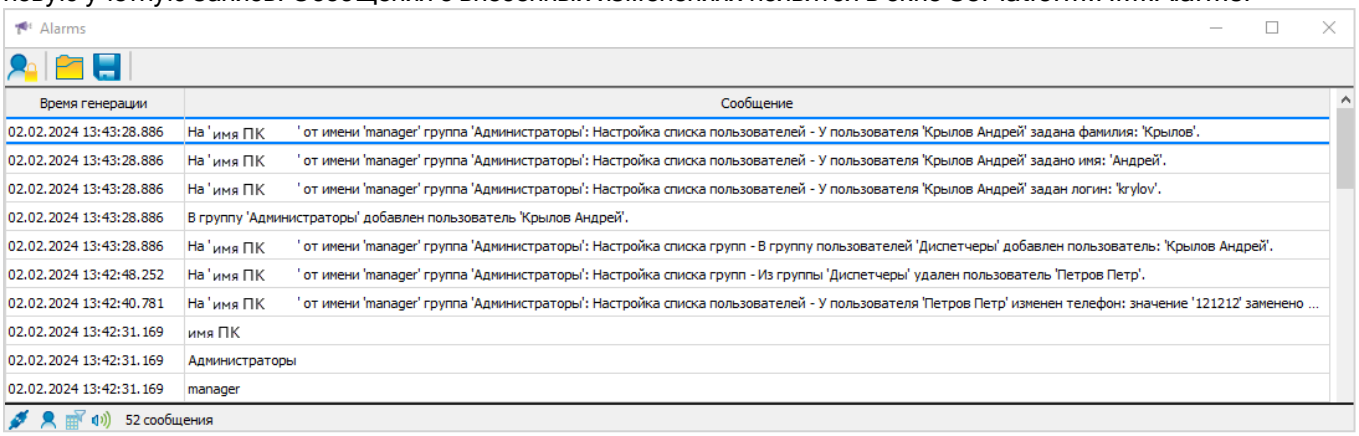


6. Постройте решение и примените конфигурацию. Чтобы убедиться, что сигналы созданы в сервере, откройте приложение Конфигуратор или Service - OPCExplorer и проверьте, что созданная папка с сигналами появилась в дереве сигналов.

Получение сообщений аудита

После внесения изменений в конфигурации сервера и агента безопасности, перезапустите их службы (сервисы). В результате будет настроена и включена трансляция сообщений аудита. Чтобы ознакомиться с результатом, используйте любое средство просмотра значений сигналов сервера или системных сообщений.

Для примера ниже приведено изображение окна приложения SePlatform.HMI.Alarms. Внесите изменения в конфигурацию SePlatform.Security: укажите номер телефона существующего пользователя или создайте новую учетную запись. Сообщения о внесенных изменениях появятся в окне SePlatform.HMI.Alarms.



8. Контроль целостности файлов и папок

Подсистема SePlatform.Security позволяет проводить проверку состояния файлов и папок на текущем компьютере. При выполнении проверки текущее состояние файлов сравнивается с ожидаемым состоянием. Ожидаемое состояние называется эталоном.

По умолчанию контроль целостности включен и выполняется для некоторых системных файлов и папок. Отключение функции контроля целостности описано ниже (стр. 93).

Чтобы изменить настройки контроля целостности, следует редактировать конфигурационные файлы `seplatform.security.agent.xml` и `seplatform.security.ic.xml`, расположенные в:

- `C:\Program Files\SePlatform\SePlatform.Security` - для ОС Windows;
- `/opt/SePlatform/SePlatform.Security` - для ОС Linux.

В конфигурационном файле `seplatform.security.ic.xml` можно указать контролируемые папки и файлы, задать таймер проверки целостности и определить серьезность нарушений целостности. Здесь же можно исключить для контролируемых папок дату последней модификации из результатов проверки.

1. Чтобы указать контролируемые папки и файлы, назначьте атрибуту `file` элемента `<IC>`, вложенного в `<ICList>`, значение, являющееся полным путем к контролируемой папке или файлу. В одном элементе `<ICList>` может быть указано несколько вложенных элементов `IC`.

ПРИМЕР

```
<SePlatform.Integrity.Control>
	<ICList>
		<IC file="C:\Windows\system32" />
		<IC file="C:\Windows\Cursors" />
	</ICList>
	<Options ICPeriodSeconds="300"/>
</SePlatform.Integrity.Control>
```

Список контролируемых файлов можно настроить.

- Можно фильтровать, какие именно файлы следует контролировать, с помощью маски. Для этого укажите значение атрибута `mask` элемента `<IC>`. Таким образом можно контролировать, например, только файлы с определенным расширением.

ПРИМЕР

```
<SePlatform.Integrity.Control>
	<ICList>
		<IC file="C:\Windows\system32" mask="*.exe;*.dll"/>
	</ICList>
	<Options ICPeriodSeconds="300"/>
</SePlatform.Integrity.Control>
```

› Можно исключить из контроля целостности все папки и файлы, вложенные в контролируемую папку. Тогда контроль целостности будет выполняться только для самой папки. Для этого укажите значение **«0»** для атрибута `recursive` элемента `<IC>`.

ПРИМЕР

```
<SePlatform.Integrity.Control>
	<ICList>
		<IC file="C:\Windows\system32" recursive="0"/>
	</ICList>
	<Options ICPeriodSeconds="300"/>
</SePlatform.Integrity.Control>
```

› Можно исключить из контроля целостности конкретный файл или папку, вложенную в контролируемую папку. Для этого укажите полный путь к исключаемым файлам и папкам в качестве значения атрибута `file` элемента `<IC>`, вложенного в элемент `<ICExclude>`. В одном элементе `<ICExclude>` может быть указано несколько вложенных элементов `IC`.

ПРИМЕР

```
<SePlatform.Integrity.Control>
	<ICList>
		<IC file="C:\Windows\Cursors"/>
	</ICList>
	 <ICExclude>
		<IC file="C:\Windows\Cursors\busy.svg"/>
	</ICExclude>
	<Options ICPeriodSeconds="300"/>
</SePlatform.Integrity.Control>
```

2. Чтобы задать таймер проверки указанных файлов, назначьте атрибуту `ICPeriodSeconds` элемента `<Options>` длительность интервала проверок в секундах. Если необходимо, чтобы проверка проводилась только по запросу пользователя, укажите атрибуту `ICPeriodSeconds` значение **«0»**.

3. Чтобы определить серьезность нарушений целостности файлов, добавьте в элемент `<Options>` новые атрибуты и назначьте им значения типа `bool`. Новыми атрибутами могут быть:

› атрибут `ICErrorObjectNotExist`, определяющий серьёзность нарушения "Объект не существует".

› атрибут `ICErrorDateChanged`, определяющий серьёзность нарушения "Изменилась дата объекта".

› атрибут `ICErrorFileChanged`, определяющий серьёзность нарушения "Изменилось содержимое файла".

› атрибут `ICErrorNewObject`, определяющий серьёзность нарушения "Обнаружен новый объект".

Если указать новому атрибуту значение `true`, то нарушение данного типа будет считаться ошибкой, если `false` - нарушение данного типа будет считаться предупреждением. По умолчанию все нарушения считаются ошибками.

Если требуется, чтобы о каждом нарушении приходило отдельное подробное сообщение, необходимо указать максимально допустимое количество таких сообщений в журнале. Укажите это количество в атрибуте `ICErrorLogMax` элемента `<Options>`. По умолчанию значение атрибута равно **«0»**.

4. При выполнении проверки целостности папки можно исключать дату последней модификации папки из результатов проверки. Это необходимо, например, когда один из вложенных в контролируемую папку файлов постоянно перезаписывается. Файл можно исключить из проверки, но в некоторых операционных системах изменение файла приводит к изменению папки, и тогда подсистема безопасности отправляет сообщение о нарушении целостности папки. Чтобы этого не происходило, элементу `<Options>` следует указать атрибут `ICCheckDirDateChanged` со значением:

   - **«false»** - чтобы дата последней модификации папки не учитывалась при проверке целостности;
   - **«true»** - чтобы дата последней модификации папки учитывалась при проверке целостности.

   Значение атрибута по умолчанию - **«true»**.

После изменения настроек контроля целостности необходимо перезапустить службу (сервис) агента безопасности. После этого с сообщениями о выполнении проверок можно ознакомиться, например, в приложении Service - LogViewer. Сообщения имеют следующий вид:

```
Проверено XXX / YYY объектов. Обнаружено нарушений AA. Ошибок A1, предупреждений A2.
Эталоном скрыто нарушений BB.
```

Здесь:

- **«XXX»** - количество файлов, которые записаны в эталон. Это число постоянно, если эталон не пересоздавать.
- **«YYY»** - фактическое количество файлов в подконтрольных папках. Контроль целостности выполняется для всех этих файлов, из которых только XXX записаны в эталон.
- **«AA»** - общее количество нарушений. Среди них:
  - **«A1»** - количество нарушений, считающихся ошибками.
  - **«A2»** - количество нарушений, считающихся предупреждениями.

  Как определить тип нарушения описано выше, в пункте 3 настройки контроля целостности.
- **«BB»** - количество файлов, к которым не удалось получить доступ на момент создания эталона. Не входят в общую статистику ошибок.

Отключение контроля целостности

Чтобы отключить функцию контроля целостности, перейдите к файлу `seplatform.security.agent.xml`. Здесь назначьте атрибуту `ICMode` элемента `<Options>` значение:

- **«0»** - для отключения контроля целостности;
- **«1»** - для включения контроля целостности.

```
<Options LoggerLevel="2" ICMode="0" ... />
```

9. Безопасность в компонентах Систэм Платформ

Подсистема безопасности SePlatform.Security позволяет разграничивать возможности пользователей в компонентах Систэм Платформ. Например, сервис безопасности можно использовать в SePlatform.HMI.Alarms, SePlatform.HMI.Trends. Подробнее о том, как активировать сервис безопасности, читайте в документах на соответствующие компоненты.

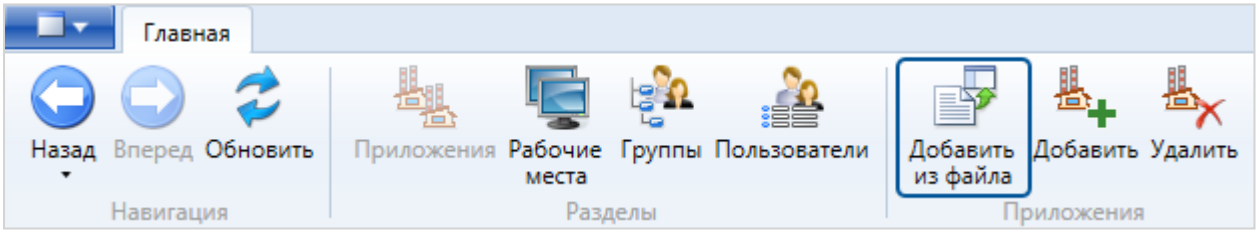
После того, как сервис безопасности активирован, необходимо назначить пользователям права на использование возможностей компонентов. Для этого необходимы приложения, содержащие эти права. Создавать приложения не нужно, используйте шаблоны приложений:

- **«Alarms»** для SePlatform.HMI.Alarms;
- **«Trends»** для SePlatform.HMI.Trends.

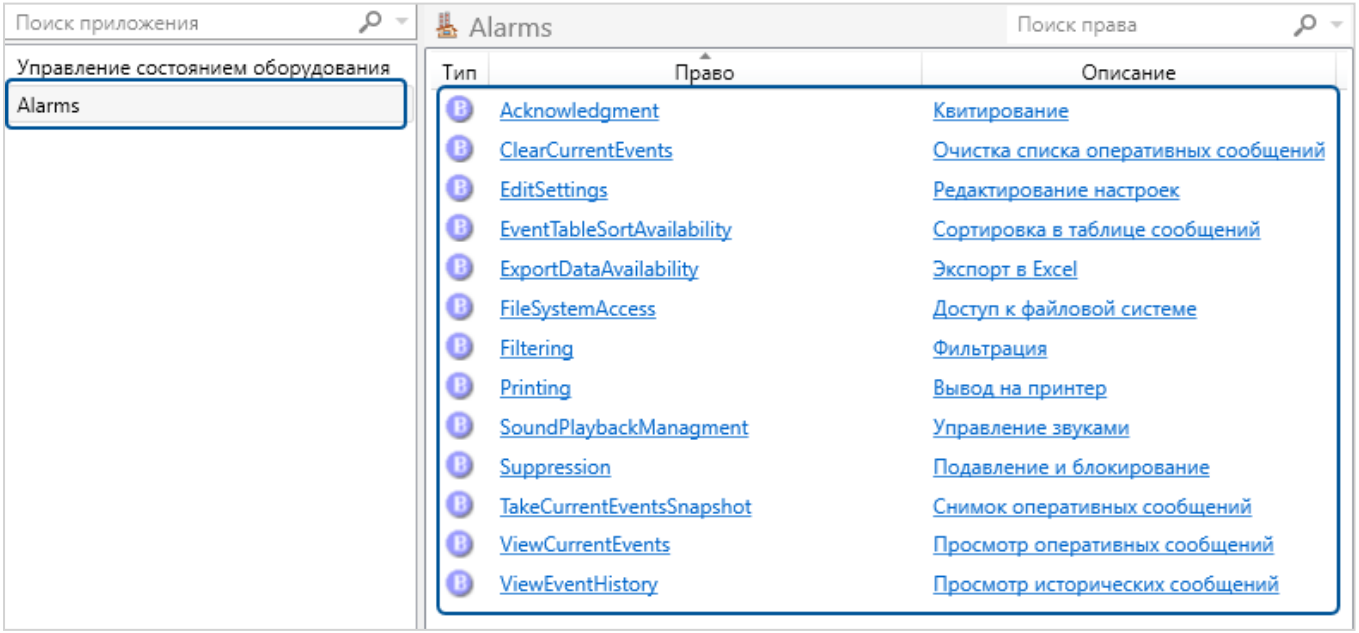
Шаблоны поставляются вместе с дистрибутивом SePlatform.Security и находятся в папке:

- `C:\Program Files\SePlatform\SePlatform.Security\Configurator\Templates` или `C:\Program Files (x86)\SePlatform\SePlatform.Security\Configurator\Templates` для ОС Windows;
- `/opt/SePlatform/SePlatform.Security/Configurator/Templates` для ОС Linux.

Чтобы использовать приложения в своих проектах, импортируйте приложения в конфигурацию SePlatform.Security. Для этого откройте окно редактирования приложений и нажмите **Добавить из файла**.



Перейдите к папке с шаблонами приложений и выберите нужный шаблон. Выбранное приложение появится в списке приложений и будет содержать права на использование возможностей компонента. Подробнее каждое право описано в документе на соответствующий продукт.



10. Решение распространенных проблем

В разделе представлены инструкции по устранению проблем, возникающих при настройке компонентов SePlatform.Security, при редактировании конфигурации на LDAP-сервере с помощью SecurityConfigurator, и в процессе работы подсистемы безопасности в целом. Раздел находится в разработке и будет дополняться. Подзаголовки раздела совпадают с текстами ошибок:

- в журнале приложений Windows;
- в приложении Service - LogViewer;
- в диалоговых окнах приложения SecurityConfigurator.

Ошибки в системных журналах или в Service - LogViewer

Служба 'SECURITYAGENT' не зарегистрирована

Эта ошибка возникает в тех случаях, когда Агент SePlatform.Security не может запуститься. При этом служба **`SePlatform.Security.Agent`** (**`seplatform.security.service`**) может находиться в статусе "выполняется". В таких случаях в первую очередь стоит проверить, что конфигурационный файл `seplatform.security.agent.xml` составлен правильно. Пример конфигурационного файла находится в Приложение А: Пример конфигурационного файла Агент SePlatform.Security (стр. 101).

Ошибка при подключении к LDAP-серверу 'x.x.x.x:x'. Операция не удалась. Код ошибки: 34

В конфигурационном файле `seplatform.security.agent.xml` каталог администратора LDAP указан в неправильном формате. Используйте формат указания каталогов, принятый для OpenLDAP: **«`cn="логин-администратора",dc="домен-базы-данных"`»**.

ПРИМЕР

Неправильно: `<LdapUser value="Manager"/>`

Правильно: `<LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>`

Ошибка при подключении к LDAP-серверу 'x.x.x.x:x'. Неверное имя пользователя или пароль

В конфигурационном файле `seplatform.security.agent.xml` указан неверный каталог администратора LDAP.

Каталог администратора LDAP зачастую создается на этапе установки OpenLDAP. Не меняйте значение, указанное в конфигурационном файле:

- для ОС Windows - `<LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>`;
- для ОС Linux - `<LdapUser value="cn=admin,dc=maxcrc,dc=com"/>`.

Неправильный пароль для подключения к LDAP / Ошибка с кодом 53

Если пароль указан верно, а ошибка все равно возникает - убедитесь, что пароль указан в зашифрованном виде, например:

```
<LdapPassword value="U7y9IEVgu3Bg++VKHxkRv4baTM6CKpuosNlqFNVJs2GVYIBKHCyx
/9omgL3DJigUPjFmX10FoNRYPeg3ycHSYLBDlOn7XXJewvulXD837Y8aQbOBfxU35AowqUR+8
yjFYFqFPxn7/fpIheuz6iuot9cJvqtrOyiMgHkFuOiRIOE"/>
```

Чтобы зашифровать пароль, используйте приложение `seplatform.security.crypter.exe`, расположенное в `C:\Program Files\SePlatform\SePlatform.Security\Utils`. Подробнее - в разделе 4. Агент безопасности и его настройка (стр. 38), в пункте Указать администратора LDAP.

Сообщения вида "<= mdb_equality_candidates: (xxx) not indexed"

Сообщения появляются в системном журнале Linux, когда OpenLDAP не индексирует указанный атрибут (xxx) для более быстрого поиска. Чтобы устранить эту проблему, необходимо присвоить индекс следующим образом:

1. В любом месте создайте файл `filename.ldif` со следующим содержимым:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: xxx eq
```

где вместо xxx следует указать атрибут из текста сообщения. Если сообщения возникают для разных атрибутов, каждый из них можно перечислить в отдельной строке вида olcDbIndex: xxx eq. Пример:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: AQRef eq
olcDbIndex: AQMemberID eq
olcDbIndex: AQMemberRole eq
```

2. Примените созданный файл с помощью команды:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f filename.ldif
```

Ошибки в диалоговых окнах приложения SecurityConfigurator

Не удалось сохранить изменения на сервере: no write access to parent. У пользователя недостаточно прав

Встречается при подключении из SecurityConfigurator, установленного на Windows, к OpenLDAP, установленному на Linux. Ошибка возникает, если не были прописаны политики контроля доступа при настройке OpenLDAP . Вернитесь на шаг : создайте файл-шаблон с описанием прав доступа к OpenLDAP и примените его.

objectClass: value #2 invalid per syntax. Неверный синтаксис

Ошибка возникает, если не была применена структура (схема) каталогов на LDAP-сервере при настройке OpenLDAP (либо была применена некорректная схема). Вернитесь на шаг .

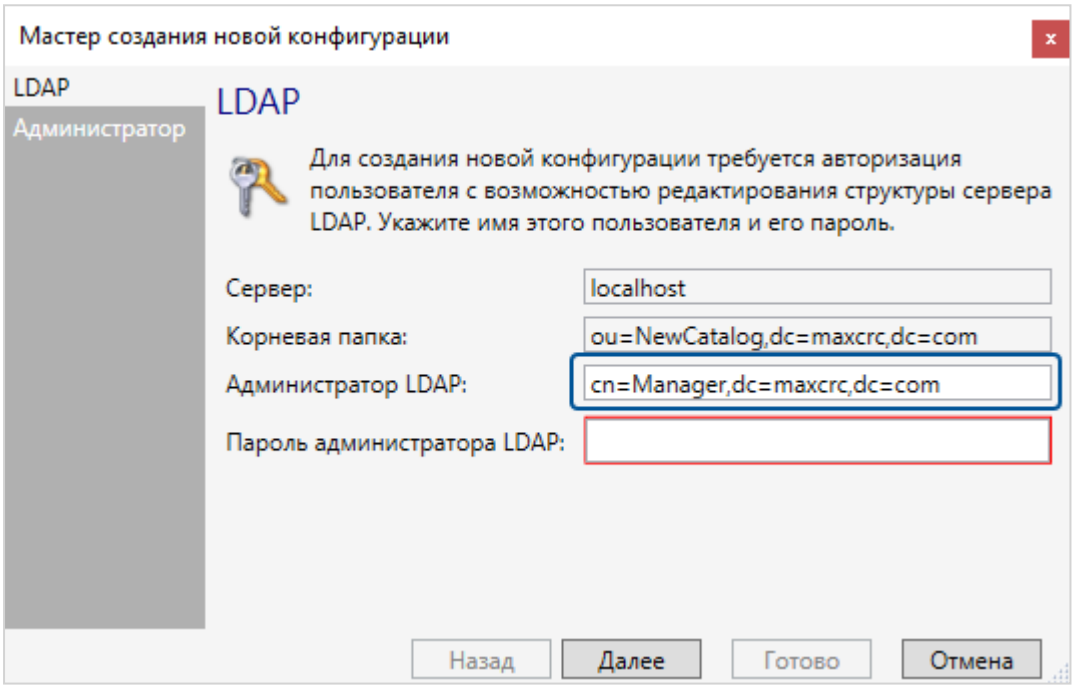
Если это не помогло, проверьте, что:

- в папке `C:\Program Files\OpenLDAP\schema` есть файл `security.schema`;
- в файле конфигурации `C:\ProgramData\OpenLDAP\openldap\slapd.conf` есть строчка:

```
include         ./schema/security.schema
```

Представленные учетные данные неверны

В этом случае следует проверить каталог администратора, указанный в мастере создания новой конфигурации SePlatform.Security, запускаемом при подключении напрямую к LDAP-серверу из SecurityConfigurator (стр. 47).



Если не меняли значение по умолчанию, то в строке **Администратор LDAP** должно быть указано:

- **«cn=Manager,dc=maxcrc,dc=com»** - если OpenLDAP установлен на Windows;
- **«cn=admin, dc=maxcrc,dc=com»** - если OpenLDAP установлен на Linux.

Объект не существует

Такая ошибка возникает, если была изменена или некорректно удалена база OpenLDAP. Проверьте, что в папке `C:\Program Files\OpenLDAP\data` находятся файлы `data.mdb` и `lock.mdb` - это и есть база. Если файлы находятся в папке, а ошибка все равно возникает, то необходимо удалить и повторно установить OpenLDAP. Обратите внимание, что это приведет к потере созданных ранее конфигураций! Поэтому попробуйте сначала найти и восстановить файлы `data.mdb` и `lock.mdb`, например, в корзине - возможно, они были удалены или перемещены по ошибке.

ОБРАТИТЕ ВНИМАНИЕ

После удаления OpenLDAP папка `C:\Program Files\OpenLDAP` остается. Если база была "сломана", то эту папку нужно удалить, иначе после повторной установки OpenLDAP будет соединяться со старой, "сломанной" базой.

Служба OpenLDAP не запускается

Следует проверить наличие конфигурационного файла `slapd.conf` в папке `C:\ProgramData\OpenLDAP\openldap`. Если файл отсутствует, то нужно скопировать туда его резервную копию из `C:\Program Files\OpenLDAP`.

Не происходит автоматический выход пользователя из системы, если длительность сессии или время бездействия истекло

Следует проверить, запущен ли сервис **`seplatform.security.useractivity.service`**. Чтобы посмотреть список запущенных сервисов, используйте команду `ps aux`. Для удобства поиска отфильтруйте результаты с помощью команды `grep`:

```
ps aux | grep seplatform.security
```

Если в списке нет нужного сервиса, необходимо вручную выполнить Запуск сервиса seplatform.security.useractivity.service.

Необходимо изменить настройки разнонаправленного резервирования OpenLDAP в ОС Linux

Чтобы изменить настройки разнонаправленного резервирования в ОС Linux, нельзя просто заново создать и применить файл `openldap-enable-syncrepl-multiprovider-server.ldif`. Сначала придется удалить прежние настройки, а затем применить новые.

Чтобы удалить прежние настройки, выполните следующие действия:

1. Выгрузите текущую конфигурацию с помощью команды:

```
sudo slapcat -b cn=config -l ldap-config.ldif
```

2. В любом текстовом редакторе измените полученный файл `ldap-config.ldif`. Например, можно использовать редактор nano:

```
sudo nano ldap-config.ldif
```

Числа, пути и названия могут отличаться от приведенных в примере ниже.

2.1. Удалите запись olcServerID:

```
olcServerID: 1
entryCSN: 20230417093406.763770Z#000000#000#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20230417093406Z
```

2.2. Удалите блок, содержащий модуль syncprov.la:

```
dn: cn=module{1},cn=config
objectClass: olcModuleList
cn: module{1}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}syncprov.la
structuralObjectClass: olcModuleList
entryUUID: be4047c6-714e-103d-91db-cbf1dc15f9bc
creatorsName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
createTimestamp: 20230417093406Z
entryCSN: 20230417093406.762126Z#000000#000#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20230417093406Z
```

2.3. Удалите блок, содержащий olcSyncrepl и olcMirrorMode:

```
olcSyncrepl: {0}rid=001 provider=ldap://1.2.3.4:389 bindmethod=simple
binddn="cn=admin,dc=maxcrc,dc=com" credentials="secret" searchbase="dc=max
crc,dc=com" scope=sub schemachecking=on type=refreshAndPersist retry="30 5
300 3" interval=00:00:05:00
olcSyncrepl: {1}rid=002 provider=ldap://1.2.3.4:389 bindmethod=simple
binddn="cn=admin,dc=maxcrc,dc=com" credentials="secret" searchbase="dc=max
crc,dc=com" scope=sub schemachecking=on type=refreshAndPersist retry="30 5
300 3" interval=00:00:05:00
olcMirrorMode: TRUE
entryCSN: 20230417093406.764528Z#000000#001#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20230417093406Z
```

2.4. Удалите блоки, содержащие olcOverlay syncprov:

```
dn: olcOverlay={0}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: {0}syncprov
olcSpSessionlog: 100
structuralObjectClass: olcSyncProvConfig
entryUUID: be407890-714e-103d-91dc-cbf1dc15f9bc
creatorsName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
createTimestamp: 20230417093406Z
entryCSN: 20230417093406.763396Z#000000#000#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20230417093406Z
```

```
dn: olcOverlay={1}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: {1}syncprov
structuralObjectClass: olcSyncProvConfig
entryUUID: be414d38-714e-103d-91dd-cbf1dc15f9bc
creatorsName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
createTimestamp: 20230417093406Z
entryCSN: 20230417093406.768839Z#000000#001#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20230417093406Z
```

3. Остановите сервис OpenLDAP, а затем убедитесь, что он остановлен:

```
sudo service slapd stop
sudo systemctl status slapd
```

4. Очистите папку от прежней конфигурации:

```
sudo rm -rf /etc/ldap/slapd.d/*
```

5. Инициализируйте очищенный от прежних настроек файл `ldap-config.ldif` в `slapd.d`:

```
sudo slapadd -b cn=config -l ldap-config.ldif -F /etc/ldap/slapd.d/
```

6. Поправьте права доступа к папке `slapd.d`:

```
sudo chown -R openldap:openldap /etc/ldap/slapd.d/
```

7. Запустите сервис OpenLDAP, а затем убедитесь, что он запущен:

```
sudo systemctl start slapd
sudo systemctl status slapd
```

Прежние настройки разнонаправленного резервирования удалены. Теперь файл `openldap-enable-syncrepl-multiprovider-server.ldif` можно создать и применить заново, как описано в разделе Разнонаправленное резервирование.

11. Приложения

Приложение А: Пример конфигурационного файла Агент SePlatform.Security

Приведенный пример конфигурации Агент SePlatform.Security описан так, что:

- точка доступа Net-агента установлена на локальной рабочей станции;
- LDAP-сервер установлен на локальной рабочей станции;
- администратором является Manager, как при умолчании;
- пользователем по умолчанию является Guest;
- трансляция аудита сообщений включена:
  - категории важности указаны как при умолчании;
  - трансляция сообщений ведется в две пары сигналов, как в примере (стр. 82);
- контроль целостности включен;
- заблокировано сочетание клавиш **«ctrl+alt+del»** и **«ctrl+shift+esc»**, как при умолчании.

```
<SePlatform.Security.Agent>
 <EntryPointNetAgent Address="127.0.0.1" Port="1010"/>

 <LdapHosts>
  <LDAPServer Address="127.0.0.1" Port="389"/>
 </LdapHosts>

 <LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>
 <LdapPassword
value="...Wq7cRi9SdqyWWWYzUuxoio7F7dLaIEDeRwlee1PlcBlpLfL17KnI..."/>

 <LdapSecure value="False"/>

 <SecurityDn value="ou=SePlatformSecurity,dc=maxcrc,dc=com"/>

 <DefaultUser value="Guest"/>
 <DefaultUserPassword value="VuZyuLC...JFchMHvKXNeztHoFpe24v2Wl9viv"/>
 <GuestDisplayName value=""/>

 <mesPrefix value=""/>

 <AuditLogConsumers TraceAudit="1">
  <OpcDaLogConsumer>
   <Server Host="127.0.0.1" Type="OPC" ProgId="SePlatform.OPCDAServer"
TCPServerPort="4388" HostTcpReserve="" MasterPasswordCipher="">
    <SeverityMap>
     <Severity Category="Critical" Value="800"/>
     <Severity Category="Important" Value="200"/>
     <Severity Category="Info" Value="100"/>
     <Severity Category="Debug" Value="0"/>
    </SeverityMap>
```

```
    <SignalMap>
     <Signal Name="Messages.DisplayNameDynamicMessage" Mode="DynamicEvent"
Type="DisplayName"/>
     <Signal Name="Messages.DisplayNameMessage" Mode="Value"
Type="DisplayName"/>
     <Signal Name="Messages.AdminDynamicMessage" Mode="DynamicEvent"
Type="Admin"/>
     <Signal Name="Messages.AdminMessage" Mode="Value" Type="Admin"/>
    </SignalMap>
   </Server>
  </OpcDaLogConsumer>
 </AuditLogConsumers>

 <Options LoggerLevel="2" ICMode="1"
kbDriverString="0x1D+0x38+0x53;0x1D+0x2A+0x01;" UseRightsCacheStorage="0" />
</SePlatform.Security.Agent>
```

Приложение B: SCAN-коды клавиш

Название клавиши	Код
Esc	0x01
Win левый	0x5B
Win правый	0x5C
Caps Lock	0x3A
Tab	0x0F
Shift левый	0x2A
Shift правый	0x36
Ctrl левый	0x1D
Ctrl правый	0x11D
Alt левый	0x38
Alt правый	0x138
F1	0x3B
F2	0x3C
F3	0x3D
F4	0x3E
F5	0x3F
F6	0x40
F7	0x41
F8	0x42
F9	0x43
F10	0x44
F11	0x57
F12	0x58
← Backspace	0x0E
Enter	0x1C
↑	0x48

Название клавиши	Код
↓	0x50
←	0x4B
→	0x4D
Пробел	0x39
PrtSc	0x54
Scroll Lock	0x46
Pause/Break	0x45
Insert	0x52
Home	0x47
Page Up	0x49
Delete	0x53
End	0x4F
Page Down	0x51
Num Lock	0x45
] }	0x1B
[{	0x1A
= +	0x0D
; :	0x27
/ ?	0x35
. >	0x34
- _	0x0C
' "	0x28
< ,	0x33
|	0x2B
A	0x1E
B	0x30
C	0x2E

Название клавиши	Код
D	0x20
E	0x12
F	0x21
G	0x22
H	0x23
I	0x17
J	0x24
K	0x25
L	0x26
M	0x32
N	0x31
O	0x18
P	0x19
Q	0x10
R	0x13
S	0x1F
T	0x14
U	0x16
V	0x2F
W	0x11
X	0x2D
Y	0x15
Z	0x2C
0	0xB
1	0x2
2	0x3
3	0x4

Название клавиши	Код
4	0x5
5	0x6
6	0x7
7	0x8
8	0x9
9	0xA

Приложение C: Параметры запуска SecurityConfigurator

Параметр	Описание и пример
`WindowsFixed`	Для главного окна приложения и его дочерних окон заблокирована возможность менять положение или размер. `seplatform.security.configurator.exe WindowsFixed`
`FileSystemSafeMode`	Управление режимом ограничения доступа к файловой системе. Блокирует возможность вызова окна справки. `seplatform.security.configurator.exe FileSystemSafeMode`
`Height`, `Width`	Размер главного окна приложения при запуске: › `Height` - высота окна; › `Width` - ширина окна. ОБРАТИТЕ ВНИМАНИЕ Если указан один параметр, второй параметр должен быть указан обязательно. `seplatform.security.configurator.exe Width 800 Height 600`
`Top`, `Left`	Положение главного окна приложения при запуске: › `Top` - расстояние от верхней границы экрана до окна; › `Left` - расстояние от левой границы экрана до окна. ОБРАТИТЕ ВНИМАНИЕ Если указан один параметр, второй параметр должен быть указан обязательно. `seplatform.security.configurator.exe Top 200 Left 100`
`SetScreen`	Номер монитора, на котором требуется отобразить главное окно приложения при запуске. Номера мониторов заданы в настройках ОС. Окно конфигуратора откроется на указанном мониторе в тех же координатах, в которых было закрыто в последний раз. `seplatform.security.configurator.exe SetScreen 2`

Параметр	Описание и пример
`AlwaysOnTop`	Главное окно приложения будет всегда отображаться поверх других окон. ПРИМЕЧАНИЕ Окно может быть перекрыто окном другого приложения Систэм Платформ (например SePlatform.HMI.Alarms), если оно тоже запущено с параметром `AlwaysOnTop`. `seplatform.security.configurator.exe AlwaysOnTop`

Приложение D: Права стандартного приложения SePlatform.Security

Право	Краткое описание	Описание
AttempsTimeOut	Таймаут при превышении количества попыток входа, мин	Длительность блокировки пользователя при превышении количества неудачных попыток, указанных в **MaxAttempsCount**.
ConfigurationAccess	Редактирование конфигурации	Предоставляет доступ к редактированию конфигурации SePlatform.Security. Этим правом наделяется администратор SePlatform.Security.
EditSettings	Изменение настроек	Предоставляет доступ к настройкам SecurityConfigurator.
InteractiveLogon	Интерактивный вход	Позволяет исключить учетную запись из списка пользователей, предоставляемого по запросу. Например: › из выпадающего списка пользователей в окне входа в конфигураторе; › из списка, запрашиваемого компонентом **Список пользователей** расширения SePlatform.HMI.Security. Ранее применялось для запрета/разрешения входа. Сейчас для этого следует использовать блокировку учетной записи пользователя (см. Заблокировать пользователя (стр. 65))
LowerCount	Количество в пароле символов в нижнем регистре	Устанавливает минимально допустимое количество символов в нижнем регистре в пароле.
MaxAttempsCount	Количество попыток входа, шт	Устанавливает количество неудачных попыток входа для пользователя. Если пользователь не войдет за указанное количество попыток, то блокируется на время, указанное в **AttempsTimeOut**. При вводе неправильного пароля Агент SePlatform.Security сообщает о количестве оставшихся попыток входа до временной блокировки.

Право	Краткое описание	Описание
MaxIdleTime	Максимальное время бездействия, мин	Устанавливает время бездействия пользователя. Таймер сбрасывается при каждом взаимодействии пользователя с АРМ - щелчком или движением мыши, вводом текста с клавиатуры и т.д. Если же за указанное время пользователь не взаимодействует с АРМ, происходит автоматический выход пользователя из системы. Эффективным значением права является максимальное значение.
NumberCount	Количество цифровых символов в пароле	Устанавливает минимально допустимое количество цифр в пароле.
PasswordAge	Срок действия пароля, дней	Устанавливает границы срока действия пароля. До истечения минимального срока действия обновить пароль нельзя. После истечения максимального срока действия пароля попытки входа со старыми учетными данными будут отклоняться. Эффективным значением минимального срока является максимальное значение. Эффективным значением максимального срока является минимальное значение.
PasswordComplexity	Сложность пароля	Обязательность использования в пароле следующих видов символов: › цифры; › буквы нижнего регистра; › буквы верхнего регистра; › специальные символы.
PasswordMinLength	Минимальная длина пароля	Устанавливает минимально допустимое количество символов в пароле.
PasswordNotifyForChange	Уведомление о смене пароля, дней	Позволяет создать напоминание об истечении срока действия пароля для пользователя. За указанное до истечения пароля время будет отправлено напоминание о скором истечении срока действия пароля. Эффективным значением является максимальное значение.
PasswordsInHistory	Количество паролей в истории	Устанавливает количество хранимых в истории паролей. Обновить пароль на такой же, как в истории паролей, не получится. Эффективным значением является максимальное значение.

<table>
<tr><th>Право</th><th>Краткое описание</th><th>Описание</th></tr>
<tr><td>SessionDurationLimit</td><td>Максимальное время сессии, мин</td><td>Устанавливает длительность сессии пользователя. После истечения указанного времени происходит автоматический выход пользователя из системы.
Эффективным значением является минимальное значение.</td></tr>
<tr><td>SpecialCount</td><td>Количество специальных символов в пароле</td><td>Устанавливает минимально допустимое количество специальных символов в пароле.
Специальные символы
<table><tr><td>?</td><td>!</td><td>@</td><td>#</td><td>$</td><td>%</td><td>^</td><td>&</td><td>№</td><td><</td><td>></td></tr><tr><td>_</td><td>-</td><td>=</td><td>+</td><td>*</td><td>(</td><td>)</td><td>[</td><td>]</td><td>{</td><td>}</td></tr><tr><td>.</td><td>,</td><td>:</td><td>;</td><td>~</td><td>`</td><td>'</td><td>"</td><td>\</td><td>|</td><td>/</td></tr></table></td></tr>
<tr><td>UpperCount</td><td>Количество в пароле символов в верхнем регистре</td><td>Устанавливает минимально допустимое количество символов в верхнем регистре в пароле.</td></tr>
<tr><td>ViewConfiguration</td><td>Просмотр конфигурации</td><td>Предоставляет доступ к просмотру конфигурации SePlatform.Security без возможности редактирования.</td></tr>
<tr><td>WinKeysShortcutAccess</td><td>Доступ к сочетаниям клавиш Windows</td><td>Предоставляет доступ к использованию сочетаний клавиш (так называемых Hotkeys).
Чтобы использовать сочетания клавиш, их необходимо настроить. Подробнее об этом в 4. Агент безопасности и его настройка (стр. 38).</td></tr>
</table>

История изменений

1.4

1.4.4

Исправления

- Устранена причина, по которой при перезапуске службы **SePlatform.Security.Agent** старые процессы не завершались. Из-за этого после перезапуска службы возникали другие проблемы:
  - не отключался файловый аудит;
  - некоторые сигналы SePlatform.Data Server, куда записывались сообщения аудита, не получали актуальных значений.
- Исправлена ошибка, из-за которой пропадало соединение между агентом безопасности и SePlatform.Net-агентом.
- При изменении значений прав в сообщениях аудита теперь отображаются как новые, так и старые значения.
- При выполнении контроля целостности файлу, который был перемещен из контролируемой папки, а затем возвращен в нее, ошибочно присваивался статус удаленного.
- В ОС Linux аудит изменений файлов теперь по умолчанию отключен.
- В ОС Linux сервисы безопасности теперь запускаются автоматически после обновления или установки SePlatform.Security.

1.4.5

Внутренние изменения. Функциональность подсистемы не изменилась.

1.4.6

Обратите внимание: не рекомендуется использовать предыдущую версию 1.4.5 из-за иногда возникающих ошибок запуска проектов SePlatform.HMI, использующих компоненты безопасности.

Исправления

- Исправлена ошибка, из-за которой результаты незамедлительной повторной проверки целостности файлов отличались от результатов предыдущей проверки.
- Устранена причина, по которой заблокированные учетные записи пользователей не разблокировались по истечении времени блокировки.

- Исправлены ошибки генерирования сообщений аудита:
  - Ранее при изменении обычного значения числового права ошибочно генерировалось два сообщения аудита - об изменении разрешенного и запрещенного значений права. Теперь генерируется одно сообщение об изменении значения права.
  - При изменении значения права **Максимальное время сессии** старое значение ошибочно отображалось в секундах вместо минут.
  - При изменении значения права **Срок действия пароля** указывалось некорректное старое значение права.
  - При изменении значения права **Срок действия пароля** для группы из нее удалялись и вновь добавлялись пользователи.
  - В некоторых сообщениях отсутствовали пробелы, что затрудняло читаемость.

1.4.7

Исправления

- Исправлена ошибка, из-за которой при запросе результата проверки целостности файлов и папок время последней проверки не обновлялось.
- Устранена причина, по которой при переводе пользователя из одной группы в другую удавалось установить его учетной записи пароль, подходящий парольным политикам прежней группы, но не новой.

1.4.9

Новая возможность

Реализована возможность указывать событиям аудита звук и необходимость квитирования. Для этого обновлены конфигурационные файлы:

- В файле `seplatform.security.agent.xml` для карты важности событий `<SeverityMap>` звук указывается в качестве значения нового атрибута `Sound`.
- В файле `seplatform.security.agent.json` для каждого шаблона сообщения звук и необходимость квитирования указываются в качестве значений параметров `sound` и `ackrequired` соответственно.

Улучшение

В файле `seplatform.security.agent.json` обновлен шаблон сообщения аудита `AUDIT_IC_CREATE_ETHALON2`, уведомляющего о создании эталона.

Исправления

- Исправлена ошибка, из-за которой для пользователя не обновлялось количество паролей в истории при переводе его из группы с назначенным правом "Количество паролей в истории" в группу без такого права.
- Устранена причина, по которой Агент SePlatform.Security не мог подписаться на сигналы для генерации сообщений аудита после перезагрузки АРМ.

1.4.10

Улучшение

В файл `seplatform.security.agent.json` добавлен новый шаблон сообщения, уведомляющего о добавлении роли пользователю.

Исправления

- Устранена причина циклической перезагрузки агента безопасности, возникавшей после удаления у текущего пользователя прав доступа к папке, целостность которой контролировалась агентом.
- Теперь при авторизации пользователя после изменения парольных политик всегда требуется сменить пароль.

1.4.12

Внутренние изменения. Функциональность подсистемы не изменилась.

1.4.14

Улучшения

- Появилась возможность исключать логин пользователя из запрашиваемого списка пользователей. Так, например, в окне входа в конфигураторе логин такого пользователя не отобразится в выпадающем списке пользователей.
- Теперь при ручном запуске проверки целостности на удаленном компьютере в локальный журнал приходит только одно сообщение аудита о запуске проверки. Ранее приходило два одинаковых сообщения - от удаленного и от локального агентов безопасности.

Исправление

Устранена причина, по которой при создании эталона на удаленном компьютере в локальном журнале отображалось сообщение о создании эталона с неправильным именем пользователя, создавшего эталон.

Изменения документации

Редакция 1

- В раздел 2. Установка и удаление (стр. 7) добавлена команда удаления настроек и резервных копий баз OpenLDAP в ОС Linux.
- В описании настройки сообщений аудита для ОС Windows и ОС Linux теперь упоминается возможность задать этим сообщениям категорию важности.
- В разделе 10. Решение распространенных проблем (стр. 95) описано, как изменить настройки разнонаправленного резервирования OpenLDAP в ОС Linux (стр. 98).
- В разделе **«Настройка компонентов» -> «Для пользователей ОС Linux»** удалено примечание о необходимости вызова команды `export |grep DISPLAY` из директории `/opt/SePlatform/SePlatform.Security`. Команду можно вызывать из любого расположения.
- В Приложение B: SCAN-коды клавиш (стр. 103) исправлен ошибочно указанный код клавиши Esc: значение **«0x21»** заменено на правильное - **«0x01»**.

Редакция 2

- Актуализировано описание настройки контроля целостности для ОС Windows и ОС Linux. Здесь же приведена расшифровка сообщений о результатах проверки целостности.
- Обновлена схема взаимодействия компонентов SePlatform.Security в разделе 1. О продукте (стр. 5).

Редакция 3

Добавлен недостающий закрывающий слеш в примерах xml-конструкций в разделах 6.7. Организация кластерного рабочего места (стр. 75) и 7. Аудит безопасности (стр. 82).

Редакция 4

В разделе 2. Установка и удаление (стр. 7) актуализированы системные требования.

Раздел "Настройка компонентов" переименован в **«Настройка компонентов SePlatform.Security»**.

В раздел **«Настройка компонентов»** добавлен подраздел, описывающий настройку Агент SePlatform.Security и OpenLDAP **«Для пользователей RPM-систем»**.

В подразделах, описывающих настройку агента безопасности:

- Описано, как транслировать сообщения из системного журнала в сообщения аудита для пользователей Debian-систем и для пользователей RPM-систем.
- Упомянута необходимость импорта настроек модулей мониторинга для пользователей Debian-систем и для пользователей RPM-систем. Без модулей мониторинга агент безопасности не будет отслеживать длительность сессий и блокировок пользователей.

В подразделе, описывающем настройку агента безопасности для пользователей ОС Windows, упомянута необходимость установки драйвера kbDriver. Драйвер необходим для корректной блокировки использования сочетаний клавиш.

Редакция 5

В подразделах, описывающих **«Настройка компонентов SePlatform.Security»** в части трансляции сообщений аудита, описана возможность указывать:

- звук, оповещающий о наступлении события определенной важности;
- звук и необходимость квитирования для каждого события отдельно.

Редакция 6

Структура документа переработана:

- Описание компонентов SePlatform.Security из раздела 1. О продукте (стр. 5) перенесено в собственные разделы: 3. LDAP-сервер и его настройка (стр. 12), 4. Агент безопасности и его настройка (стр. 38), 6. Редактирование конфигурации на LDAP-сервере с помощью SecurityConfigurator (стр. 46). Информация из бывшего раздела "Настройка компонентов SePlatform.Security" также перенесена в эти разделы.
- Описание процесса подключения к LDAP-серверу из раздела 6. Редактирование конфигурации на LDAP-сервере с помощью SecurityConfigurator (стр. 46) вынесено в собственный подраздел 6.1. Подключение к LDAP-серверу из SecurityConfigurator (стр. 47).
- Настройки и использование аудита безопасности и контроля целостности теперь описаны в собственных подразделах 7. Аудит безопасности (стр. 82) и 8. Контроль целостности файлов и папок (стр. 91). Ранее эти функции были описаны в разделах, описывающих настройку агента безопасности.

В разделе 2. Установка и удаление (стр. 7) актуализированы системные требования.

В разделе 4. Агент безопасности и его настройка (стр. 38) описана возможность скрытия учетной записи пользователя из запрашиваемого списка пользователей.

1.3

1.3.5

Улучшения

- Ускорено выполнение контроля целостности для большого количества файлов.
- Теперь каждому сообщению аудита можно задать категорию важности. Сообщения и их категории важности описываются в файле `seplatform.security.agent.json`, расположенном в папке установки SePlatform.Security.

Исправления

- Устранена причина, по которой пропадало соединение SePlatform.HMI с Агент SePlatform.Security. Проблема возникала после выхода и повторного входа пользователя в ОС, с последующей сменой пользователя SePlatform.Security из проекта SePlatform.HMI.
- Решена проблема, из-за которой в ОС Linux не происходил автоматический выход пользователя из подсистемы безопасности по истечении:
  - времени блокировки при превышении количества неуспешных попыток входа;
  - максимального времени бездействия пользователя.

Изменения документации

Редакция 2

В схеме взаимодействия компонентов SePlatform.Security актуализирована иконка конфигуратора.
В разделе **«Настройка компонентов»**:

- Приведены новые параметры описания сервера-потребителя сообщений аудита `HostTcpReserve` и `MasterPasswordCipher` - для пользователей Windows и для пользователей Linux.
- Описана настройка списка файлов, целостность которых должна контролироваться подсистемой безопасности - для пользователей Windows и для пользователей Linux. Теперь из списка можно исключать вложенные файлы и папки, а также фильтровать контролируемые файлы и папки по расширению или названию.
- Для пользователей ОС Linux описана настройка сервиса SePlatform.Security, предназначенного для отслеживания длительности сессий и времени бездействия пользователей.

Редакция 3

В разделе **«Настройка компонентов»** -> **«Для пользователей ОС Linux»**:

- описана настройка OpenLDAP, применяемая для отслеживания длительности сессий и блокировок пользователей - импорт настроек модуля мониторинга;
- описана возможность запуска сервисов агента безопасности от имени непривилегированного пользователя.

В разделе 10. Решение распространенных проблем (стр. 95) описано, как предотвратить появление в журнале сообщений вида <= mdb_equality_candidates: (xxx) not indexed.

Во всем документе актуализированы скриншоты.